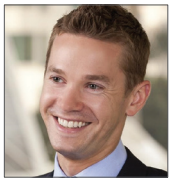
Mapping an FCPA Strategy

Internal Investigations and Enforcement Proceedings

In today's globalized economy, companies face heightened scrutiny and significant liability risks under the Foreign Corrupt Practices Act (FCPA). Even with robust compliance processes in place, companies and their counsel must be prepared for an FCPA-related eventuality.

DAVID J. SCHINDLER
PARTNER
LATHAM & WATKINS LLP

David was co-chair of the firm's White Collar Defense and Investigations Practice for over ten years. His practice focuses on white collar and government investigations, healthcare fraud and abuse, intellectual property, e-commerce, business litigation and civil litigation. David has conducted internal investigations and represented companies, boards and individuals in connection with a wide array of criminal, quasi-criminal and regulatory matters, including dozens of FCPA-related investigations around the world.



MICHAEL A. LUNDBERG
ASSOCIATE
LATHAM & WATKINS LLP

Michael's practice focuses on white collar investigations, FCPA, anti-money laundering, and securities and professional liability matters. He has represented clients from a broad range of industries on various issues, including FCPA investigations and developing anti-bribery policies, procedures and training materials. Prior to practicing law, Michael investigated conflict resource exploitation and arms trafficking in West Africa for a London-based NGO.

CONTACT

David J. Schindler

Partner, Los Angeles

O +1.213.891.8415
M +1.213.215.6663
E david.schindler@lw.com

Michael A. Lundberg

Associate, Los Angeles

O +1.213.891.8882
M +1.323.449.2888
E michael.lundberg@lw.com

More than 2,100 Lawyers Located Around the Globe

North America
Boston
Century City
Chicago
Houston
Los Angeles
New York
Orange County
San Diego
San Francisco
Silicon Valley
Washington, D.C.

Europe
Barcelona
Brussels
Düsseldorf
Frankfurt
Hamburg
London
Madrid
Milan
Moscow
Munich
Paris
Rome

Middle East
Abu Dhabi
Dubai
Riyadh

Asia
Beijing
Hong Kong
Shanghai
Singapore
Tokyo

FCPA enforcement continues to be a high priority for the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC). Both the DOJ and SEC have units dedicated to FCPA enforcement. In the last two years, they have collected over $2.1 billion in FCPA-related fines and forfeitures, and show no signs of letting up on their high-profile inquiries (see *Box, Notable Recent Settlements*). Additionally, other plaintiffs, such as shareholders, foreign governments, competitors and multilateral development banks (MDBs), continue to pursue legal actions based on FCPA-related facts.

With the substantial fines and onerous compliance requirements that can result from FCPA violations, it is critical for companies to maintain proactive compliance programs and perform regular risk assessments to avoid a potentially enterprise-threatening fate. But even with robust processes in place, companies still face intense scrutiny and must prepare strategically for an FCPA-related eventuality. This article examines:

- Best practices for conducting an effective internal investigation of an FCPA matter.
- Issues related to disclosing an internal investigation's findings to the company's board of directors or the government.
- Remedial actions a company can take in response to information uncovered during an internal investigation.
- Possible exceptions and defenses to FCPA liability.
- Key considerations in resolving an FCPA government enforcement action.
- The types of follow-on litigation that can arise after and based on a government investigation.

Search The Foreign Corrupt Practices Act: Overview for information on the activities prohibited by the FCPA, who is covered by it and penalties for violating the FCPA.

Search Foreign Corrupt Practices Act Compliance Checklist for information on developing a strong compliance program.

CONDUCTING AN INTERNAL INVESTIGATION

FCPA internal investigations often begin with facts gathered by compliance personnel in response to hotline messages or internal audit findings. As soon as a company becomes aware of a potential FCPA violation, it should notify its attorneys. In deciding whether an investigation is warranted, counsel should consider the unique circumstances of the case, such as the scope of the alleged misconduct, the materiality of the amounts at issue and the involvement of upper management. These factors also will help drive decisions during the investigation process, which includes:

- Determining who will lead the investigation.
- Protecting the attorney-client privilege.
- Defining the scope of the investigation.
- Addressing e-discovery issues.
- Analyzing financial records.
- Conducting employee interviews.

Search Conducting Internal Investigations Toolkit for a collection of resources to help companies prepare for and conduct an effective internal investigation.

DETERMINING WHO SHOULD LEAD

When a company is alerted to a potential FCPA violation, counsel should first focus on assessing whether the conduct at issue raises a legitimate concern, and is not, for example, based only on an unsubstantiated complaint from a disgruntled employee. At this stage, in-house counsel should conduct a review of the matter and make this determination.

If the allegations warrant an internal investigation, the company must consider whether the investigation should be managed by outside counsel, including whether independent outside counsel should be brought in to supervise. An investigation conducted by outside counsel, though more costly, can help:

- Provide assurance to the government that it can rely on the results of the investigation if the client decides to self-report.
- Strengthen the attorney-client privilege (see below *Protecting the Attorney-Client Privilege*).
- Avoid suggestions of undue influence by employees.
- Allow in-house counsel to return to their day jobs.

PROTECTING THE ATTORNEY-CLIENT PRIVILEGE

Before an investigation begins, a company should build protocols into its internal controls to help it preserve the attorney-client privilege, both with in-house and outside counsel. Because the investigation may involve multiple law firms from different countries, an army of forensic consultants and teams of document reviewers, among others, setting and following basic precautions is key. In particular, counsel and the company should:

- Determine who is the client for the investigation. In some instances, it may be the company, while in others, it may be the audit committee.
- Document that the purpose of the attorneys' involvement is to provide legal advice on certain key issues.
- Provide specific instructions to any relevant parties indicating that all internal investigations will be initiated and directed by attorneys for the purpose of obtaining legal advice, not for a routine business review, and regularly remind parties of this point.
- Document that any non-attorneys who have been delegated investigative responsibilities work at the direction of, and report their findings to, only designated attorneys.
- Clarify the responsibilities of personnel who hold both legal and non-legal job responsibilities. Because compliance personnel often are attorneys who perform other business functions, unclear dual roles may lead to questions about whether their communications are privileged. The government has grown increasingly uncomfortable with efforts to invoke privilege over traditional compliance work.
- Give *Upjohn* warnings at all witness interviews, notifying employees that counsel represents only the company and not the employees individually, and caution interviewees that they should keep the discussions confidential. Document these warnings in contemporaneous notes. (For more information on *Upjohn* warnings, search Attorney-Client Privilege: Identifying the Attorney and the Client on our website.)
- Mark all investigation-related documents and communications as attorney-client privileged, attorney work product, or both, as appropriate.

- Clarify which personnel will have access to investigative findings and notes, and carefully restrict access and information distribution to only those parties.
- Understand that rules of privilege and work product protections are different in foreign jurisdictions and become familiar with relevant choice-of-law issues. In cross-border investigations, counsel should not assume that communications and documents that would ordinarily be privileged in the US are protected if deemed to be governed by a foreign jurisdiction's rules.

Search Internal Investigations: US Privilege and Work Product Protection for more on how counsel can ensure the proper creation and maintenance of the attorney-client privilege and work product protection.

Search Memorandum to Employees Regarding Proper Maintenance of the Attorney-Client Privilege for a sample memorandum from in-house counsel to company employees, with explanatory notes and drafting tips.

DEFINING THE SCOPE

FCPA internal investigations can quickly become expensive, particularly because data collection and processing, forensic accounting review, translations, travel and compliance program improvements are likely to occur across multiple jurisdictions. For example, Wal-Mart reportedly spent over $439 million in professional fees just in 2013 and 2014 on its FCPA investigations and compliance efforts.

To control the scope of an investigation, counsel should:

- **Conduct an initial risk assessment.** The risk assessment helps determine the preliminary scope of the investigation and should be adjusted periodically as new facts are gathered.
- **Build a detailed work plan.** The plan should:
  - include specific tasks and deadlines;
  - identify responsible personnel, along with reporting lines for counsel, the client and key vendor contacts; and
  - incorporate regular update meetings to ensure that progress is tracked and efforts are focused only on key items.
- **Obtain early support from executives.** Gaining the support of executives overseeing the investigation and its budget helps reinforce an adequate "tone at the top" and promote employees' cooperation with the investigative team.
- **Ensure consultants' budgets and scopes are clear.** Counsel should designate a person to monitor consultants' progress, and control budgets and any proposed scope expansion. Consultants should work at the direction of outside counsel to help protect privilege, but counsel should be extremely careful in communications with outside consultants because the claim of privilege over these communications generally are weaker than with the company's employees.

ADDRESSING E-DISCOVERY ISSUES

The complexity of collecting, processing and reviewing relevant electronic data is compounded in an FCPA internal investigation due to the different jurisdictions at play. Knowing what data is available, where it is located and whether it can be accessed legally is paramount. Therefore, depending on the anticipated scope of the investigation, counsel may suggest that the company consider hiring an experienced forensic data vendor with international experience and local capability in the jurisdictions at issue.

Additionally, counsel should advise the company promptly to issue a litigation hold in each location where potentially relevant documents or information exist.

Search Litigation Hold Toolkit for a collection of resources on when and how to issue a litigation hold, including model documents with explanatory notes and drafting tips.

Finally, before initiating any discovery in connection with the investigation, counsel and the client should review and update the company's electronic data policies and procedures, and discuss the following key issues:

- **The types of data that might hold information useful to the investigation.** This includes, for example, standard electronic documents, e-mails, voicemails, instant messages and conversations via texting applications, such as WhatsApp.
- **The location of data and the client's data storage architecture.** This includes, for example, the physical location of servers, backup tapes, returned laptops, external hard drives and cloud storage facilities.
- **Data retention, backup and deletion protocols.** This includes the protocols for network servers, shared drives, personal folders, employee laptops and handheld devices.
- **Which jurisdictions are implicated and the applicable laws.** Some jurisdictions have strict data privacy laws or blocking statutes. For example, counsel should be careful about collecting and reviewing data from China, where even routine financial data may be considered a "state secret."
- **Whether to hire an e-discovery vendor.** The risks of a client collecting and processing its own data are many, including possible allegations of incomplete and biased collection and spoliation of evidence. Depending on the scope of the investigation, counsel should consider advising the client to hire an experienced vendor, trained to conduct thorough collections, preserve metadata and avoid violating data privacy laws.
- **Whether to hire a vendor that specializes in pre-processing data.** Especially useful in processing large amounts of documents, these vendors can help identify key terms, code words, conversation patterns and potentially responsive documents across multiple languages. They can also significantly reduce the size of the review, for example, by identifying patterns of automatic or spam e-mails and removing those documents as unresponsive. In appropriate circumstances, counsel should consider hiring this type of vendor if it would lead to a more targeted and efficient data collection and review. When selecting an e-discovery vendor, counsel should inquire about its pre-processing capabilities.
- **Attorney-client privilege issues.** To protect privilege, the vendors' contracts should state that the vendor will act only at the direction of counsel.

SEC Administrative Proceedings

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 granted the SEC authority to impose civil monetary penalties through administrative proceedings, in addition to cease-and-desist orders. Initially, the SEC used administrative proceedings infrequently and for straightforward cases. However, the SEC increasingly has relied on the administrative process to resolve complex FCPA-related matters, and has announced its intention to continue doing so. In 2014, the SEC settled eight FCPA-related actions through administrative proceedings.

Administrative proceedings afford fewer rights to respondents than those in the federal courts, resulting in significant disadvantages. For example:

- The proceedings must be completed on an expedited schedule before an administrative law judge (ALJ) appointed by the SEC, who must render a decision within one year. This timeline poses a challenge in factually complex FCPA matters, and may pressure a company into settling rather than attempting to develop an exculpatory factual record.
- Although the SEC can conduct its normal investigations and subpoena witnesses, respondents have minimal power to conduct document discovery and compel witness testimony.
- The SEC can overturn the ALJ's finding, and the respondent may appeal to a circuit court of appeals for relief only after the SEC issues its final ruling.

Given this trend, counsel should consider advising companies to begin fact-finding and developing a legal strategy as soon as possible after discovery of any potential FCPA violation.

ANALYZING FINANCIAL RECORDS

FCPA internal investigations often turn on finding evidence of improper payments hidden in a mountain of financial data. Hiring an outside forensic accountant to design a protocol for collecting, sampling and searching financial records often saves time and improves accuracy. The vendor should not be the company's regular outside accounting or auditing firm. Also, to preserve privilege, the vendor's contract should state that the vendor will act only at the direction of counsel. Forensic firms sometimes can perform both the electronic document collection and the forensic accounting work.

CONDUCTING EMPLOYEE INTERVIEWS

FCPA internal investigations depend largely on what employees knew, when they knew it and their mental state at the time.

Interviewing key employees, especially those suspected of misconduct, is fraught with privilege issues and can require a mix of strategy and psychology to be effective. Counsel and the client should consider the following before interviewing employees:

- Which current or former employees are suspected of wrongdoing, who may have useful information and how to prioritize the interviews.
- Identifying documents to refresh a witness's recollection or test the truthfulness of his statements.
- Whether, to prevent collaboration on answers, counsel and the client should:
  - hold surprise interviews instead of scheduling them in advance; or
  - hold simultaneous interviews when multiple employees are suspected of collaborating in wrongdoing.
- Whether to have local counsel conduct the interviews in the local language or use outside counsel and a translator.
- Ensuring that *Upjohn* warnings are clear and documented in counsel's contemporaneous notes.
- Informing interviewees of the legal purpose of the inquiry and privileged nature of the conversation, and requesting that they keep the discussions confidential. However, it is prudent to assume that the occurrence and content of the interviews will spread quickly throughout the organization.
- Understanding the employees' rights under their contracts with the company, the company's by-laws or under foreign or local law. For example, companies may be required to provide separate counsel to employees whose conduct is at issue if those employees request separate counsel. Similarly, some foreign jurisdictions impose restrictions on a company's ability to interview employees.
- Ensuring that counsel creates and preserves detailed, contemporaneous interview notes.

Search Letter to Employee Requesting Participation in Internal Investigation for a model letter from the company to an employee, with explanatory notes and drafting tips.

DISCLOSING A KNOWN OR POTENTIAL VIOLATION

Once counsel concludes an internal investigation, counsel must determine whether, how and to whom to disclose the findings. While disclosure to the company's board of directors and outside auditors typically is required as a matter of corporate governance, whether or not to make a disclosure to the government raises separate questions. Counsel should always keep detailed records of their findings, including "hot" documents, chronologies and witness interviews.

INTERNAL DISCLOSURES

When preparing to present the investigation findings to the company's board or audit committee, counsel should bear in mind that the presentation materials could end up being disclosed to the government or, even worse, a reporter. To mitigate risk, rather than circulating a detailed memorandum setting out the legal and factual findings, counsel should

consider using a high-level summary or PowerPoint presentation supplemented by oral commentary.

EXTERNAL DISCLOSURES

The DOJ and SEC have long encouraged companies to timely disclose any FCPA violation and cooperate during the government investigation process (see below *Cooperation*). The decisions of whether, when and how to self-report to the government or the investing public, however, should be made carefully, weighing all potential benefits and drawbacks. Counsel should consider numerous factors, including:

- The seriousness of the misconduct.
- The materiality of the amounts paid to the foreign official and the materiality of any contracts arguably tainted by the payments at issue.
- Whether the misconduct was endorsed by top executives or merely a rogue sales agent.
- Whether the government is likely to find out about the misconduct through its own investigations or a whistleblower.
- Whether the disclosure and potential government investigation is likely to subject the company to follow-on civil litigation (see below *Follow-on Litigation*).
- That self-reporting almost always triggers a formal government investigation, which may be expansive and costly, especially if the scope of the misconduct is not fully understood.

In cases of minor violations by rogue actors, companies often will choose to investigate and self-remediate, carefully documenting their work. In cases of more serious misconduct, companies that self-report early, work on fixing the problem and cooperate in the government's investigation often are rewarded by lesser fines and avoiding charges.

If counsel and the client decide self-reporting is the best route to take, however, they should consider the possible privilege implications, as well as any relevant requirements under the Sarbanes-Oxley Act of 2002 (SOX).

Privilege Waivers

Counsel should try to obtain confidentiality agreements from the government and restrict any discussions to non-privileged information. If it makes strategic sense to share certain privileged information with the government, counsel should strive to share as little as possible, and simultaneously warn the client that it may face privilege waiver issues later on with third-party litigants. The selective waiver doctrine, under which a party may attempt to disclose privileged communications to the government while asserting the privilege protection against other parties, has been rejected by every federal circuit court of appeals to review the issue except for the US Court of Appeals for the Eighth Circuit (see, for example, *In re Pac. Pictures Corp., 679 F.3d 1121, 1127-28 (9th Cir. 2012)* (rejecting selective waiver doctrine); *Westinghouse Elec. Corp. v. Republic of the Philippines, 951 F.2d 1414, 1425-26 (3d Cir. 1991)* (same); but see *Diversified Indus., Inc. v. Meredith, 572 F.2d 596, 610-11 (8th Cir. 1977)* (adopting selecting waiver doctrine)).

Search Attorney-Client Privilege: Waiving the Privilege for more on the selective waiver doctrine and other waiver issues.

SOX Requirements

Counsel should take into account that public companies are subject to SOX disclosure and internal control requirements. SOX requires that a company's chief executive officer and chief financial officer make certain certifications regarding the accuracy of the company's quarterly reports and the effectiveness of the company's internal controls.

Search Internal Control Over Financial Reporting for Counsel: Why Should You Care? for more on SOX certification requirements.

Public companies also must be transparent and candid when providing information to their outside public accountants to avoid creating additional issues. Many standard audit checklists and management representation letters, which confirm in writing the accuracy of the information a company provides to its auditor, contain provisions relating to FCPA compliance.

Of course, not every FCPA violation constitutes a material failing of internal controls or pending legal proceeding requiring public disclosure. Nevertheless, a company may want to disclose risk factors regarding any geographical or sector-specific FCPA compliance risks that it faces and note its ongoing compliance efforts. These disclosures can help diffuse later claims that the company failed to alert investors of information regarding material FCPA risks or that management failed to supervise the company's compliance program.

REMEDIAL ACTIONS

Following an FCPA internal investigation, counsel and the client should assess whether there are any corrective steps that can be taken in light of the information uncovered, such as:

- Enhancing the company's FCPA compliance program.
- Disciplining employees for misconduct.
- Addressing third-party violations.

ENHANCING COMPLIANCE PROGRAMS

Anytime an FCPA-related issue triggers an investigation, counsel should advise the company to:

- Review the adequacy of its compliance program.
- Consider and adopt improvements that will make the compliance program more effective, including, for example:
  - specifying the types and (very limited) monetary amounts for gifts, entertainment and other expenses that its employees may provide to foreign officials;
  - implementing internal controls designed to detect conduct that potentially violates the FCPA and which should be difficult to circumvent; and
  - implementing a mechanism for confidential reporting of suspected violations and a process for investigating the reports.

- Circulate additional compliance messaging.
- Conduct targeted training.

Counsel should document these actions, because the company's response, or lack of response, to an FCPA concern will be an important issue during any future litigation.

Search Foreign Corrupt Practices Act Compliance Checklist and Foreign Corrupt Practices Act Anti-Corruption Policy for more on effective compliance programs.

Search Foreign Corrupt Practices Act Training for Employees: Presentation Materials for a PowerPoint presentation that can be used to train employees on their compliance obligations.

DISCIPLINING EMPLOYEES

Whether and how to discipline an employee for a suspected or known FCPA violation depends on many factors, including the severity of the violation and whether the employee's actions were legal under the local law and the company's code of conduct. If counsel and the client decide to pursue this course of action, they should:

- Consider hiring local employment counsel, because labor laws in some countries can make it difficult or impossible to terminate an employee, even for gross misconduct.
- Review the local law and the employment contract, and consider all forms of discipline, including:
  - termination;
  - demotion;
  - time off without pay;
  - permanent personnel file notes; and
  - other penalties that, when coupled with additional training, might correct the behavior and deter other misconduct.
- Document all steps taken in the process, to be able to use in a possible employment litigation and to answer any future questions from the government about the adequacy of the response to the misconduct.

Search Best Practices for Employee Discipline Checklist for more on disciplining employees for unlawful activity.

ADDRESSING THIRD-PARTY VIOLATIONS

Often, a third-party agent or consultant generates FCPA liability. Depending on the contract terms and the third party's role in a project, terminating the third party may be highly impracticable. Before taking any action, counsel should assess the situation thoroughly, including the reasons the client would provide to government authorities for the decision to retain or terminate the third party.

Ideally, the client would have set a strong tone of compliance to help shield itself from FCPA liability through third parties, including effective due diligence measures and contractual safeguards. But even if this is not the case, a company facing an FCPA violation should consider taking the following steps:

- Demand indemnification and compensation for all damages arising from the third party's violation.
- Require the third party to provide annual certifications documenting compliance with all applicable anti-corruption laws in relation to its engagement.
- Require the third party to implement an appropriate anti-corruption compliance program for all of the third party's employees who are working on the project.
- Insert contractual language that allows for:
  - financial audits;
  - immediate termination of the contract without penalty for violations of the company's anti-corruption policies;
  - indemnification for compliance-related violations; and
  - additional representations, warranties and affirmative covenants regarding anti-corruption compliance.
- Circulate a list of known third parties that pose a great compliance risk.

Search Policy for the Use of Third-party Agents Outside of the United States for a sample company policy governing the engagement of third parties, with explanatory notes and drafting tips.

EXCEPTIONS AND DEFENSES

A company may avoid FCPA liability by showing that the case falls within certain exceptions or defenses, such as:

- Actions brought outside the statute of limitations.
- Reasonable and bona fide expenditures.
- Facilitating payments.
- Payments made under duress.
- Payments permitted by local law.
- Pre-acquisition violations made by a target company.

STATUTE OF LIMITATIONS

The FCPA's anti-bribery and accounting provisions do not provide a specific statute of limitations. Therefore, the general five-year limitations period applies to both criminal and civil violations (see *18 U.S.C. § 3282*; *28 U.S.C. § 2462*). However, counsel should keep in mind that this limitations period may be extended under certain circumstances, for example:

- Cases involving allegations of ongoing or tangentially-related conduct.
- Civil cases where the defendant remained outside the US during the five-year period, even if service was possible under the Hague Service Convention. Recent court decisions have held that the limitations period may be tolled in these situations (see, for example, *SEC v. Straub, 921 F. Supp. 2d 244, 259-61 (S.D.N.Y. 2013)*).

REASONABLE AND BONA FIDE EXPENDITURES

The FCPA is not intended to halt all forms of business hospitality. It allows for reasonable and bona fide business expenditures, such as for travel and lodging, that are directly related to the promotion, demonstration or explanation of products or services, or the execution or performance of a contract with a foreign government or agency (*15 U.S.C. §§ 78dd-1(c)(2), 78dd-2(c)(2), 78dd-3(c)(2)*).

Notable Recent Settlements

In 2014, the cost of resolving an FCPA enforcement action continued to rise, with multiple high-profile settlements exceeding $100 million. For example:

- Alcoa Inc., a New-York based aluminium producer, paid $384 million in penalties to the DOJ and SEC in connection with bribes paid to Bahraini officials to influence contract negotiations between Alcoa and a government-operated aluminium plant. This is the sixth-largest FCPA enforcement settlement to date. (See *SEC Press Release, SEC Charges Alcoa With FCPA Violations (Jan. 9, 2014)*, available at *sec.gov*.)
- Avon Products Inc., a New York-based cosmetics company, and its Chinese subsidiary paid a combined $135 million in penalties to the DOJ and SEC in connection with bribes paid to Chinese officials to secure various business benefits (see *SEC Press Release, Avon Entities to Pay $135 Million to Settle SEC and Criminal Cases (Dec. 17, 2014)*, available at *sec.gov*). Avon also reportedly spent over $344 million in professional fees on its wide-ranging investigation and compliance program improvements.
- Hewlett-Packard Co., a California-based technology company, and its subsidiaries in Russia, Poland and Mexico paid $108 million in penalties to the DOJ and SEC in connection with bribes paid to foreign officials for the purpose of obtaining contracts in those countries (see *SEC Press Release, Company to Pay $108 Million to Settle Civil and Criminal Cases (Apr. 9, 2014)*, available at *sec.gov*).

To ensure that these payments are justifiable, and generally to prevent expense account abuse, companies should develop gift, entertainment and travel policies, and accompanying internal controls. This includes:

- A specific process for documenting expense requests and approvals, with extra approvals required for expenses involving government officials.
- A clear prohibition on all expenses that are lavish or excessive, or that are primarily for personal entertainment.
- Consistent application of the expense policy to employees and non-employees.
- Accurate recording of expenses in the company's financial books and records.
- Periodic auditing of expenses to identify potential risks, particularly for employees who most often entertain third parties as well as those third parties who are most often entertained.

FACILITATING PAYMENTS

Facilitating or "grease" payments refer to small amounts paid to government officials to expedite or secure the performance of a routine governmental action. "Routine governmental actions" include services that would not require an official to exercise his discretion, such as processing visas and scheduling inspections. (See *15 U.S.C. § 78dd-1(b), (f)(3)*.)

The facilitating payments exception to the FCPA is construed narrowly. The difference between a facilitating payment and a bribe can be murky. Facilitating payments are usually illegal under local law and they are explicitly prohibited under anti-bribery regimes in key countries like the UK. Further, these payments are not often documented by receipts and therefore are easy to mischaracterize. For these reasons, most global companies prohibit them entirely.

Companies that allow facilitating payments should enact internal controls to ensure they are recorded properly and help mitigate the associated risks. For example, companies can:

- Establish a general ledger code dedicated to facilitating payments.
- Train at-risk employees on how to record facilitating payments.
- Limit the amount of a single facilitating payment.
- Conduct periodic audits for accuracy.

PAYMENTS MADE UNDER DURESS

The government has stated clearly that payments made under a threat of imminent physical harm do not give rise to FCPA liability because the giver is not making the payment with corrupt intent. However, companies operating in violence-prone areas should consider implementing the following controls, among others, to help avoid an FCPA violation:

- Conduct regular security assessments to determine how employees can best avoid situations that may involve duress payments.
- Develop written policies and guidelines, and train at-risk employees.
- If possible, require that employees inform compliance personnel and seek formal, documented pre-approval before making a payment. If advance authorization is impossible, then the incident should be documented thoroughly in a memo and sent to compliance afterward for review.
- Accurately account for each duress payment. As with facilitating payments, to help prevent an inadvertent books and records violation, companies can establish a separate general ledger code dedicated to duress payments, train at-risk employees on how to record these payments and conduct periodic audits.

PAYMENTS PERMITTED BY LOCAL LAW

The FCPA does not prohibit payments that are lawful under the written laws and regulations of the foreign official's country (*15 U.S.C. §§ 78dd-1(c)(1), 78dd-2(c)(1), 78dd-3(c)(1)*). Because the rule must be written, longstanding business customs, cultural norms and a country's failure to enforce the law are all insufficient to invoke this affirmative defense.

PRE-ACQUISITION VIOLATIONS

Last year, the DOJ issued an Opinion Procedure Release indicating that the pre-acquisition activities of a target company will not generate FCPA liability for the acquiring entity if the target was not subject to the FCPA at the time the activities occurred. In other words, "[s]uccessor liability does not ... create liability where none existed before." (See *DOJ Criminal Division, Opinion Procedure Release, No. 14-02, Foreign Corrupt Practices Review, at 3 (Nov. 7, 2014)* (citation omitted), available at *justice.gov*.)

Search DOJ: Mere Acquisition of Foreign Company Does Not Retroactively Create FCPA Liability for Acquiror for more on the DOJ's Opinion Procedure Release.

- Discuss with counsel whether self-reporting to the government or shareholders is necessary.

Search M&A Due Diligence: Assessing Compliance and Corruption Risk for more on analyzing a target company's corruption risk.

RESOLVING ENFORCEMENT ACTIONS

An FCPA government enforcement action can be resolved in multiple ways. Counsel involved in these proceedings should consider:

- The different types of potential resolutions with the government.
- The impact on the client of cooperating with the government.
- Issues related to compliance experts.

Whether the company has run a thorough and honest internal investigation, presented the facts fairly and reacted adequately will be crucial in defending allegations of wrongdoing and reaching the best possible resolution.

However, to uncover any previous misconduct by the target company and, more importantly, to prevent it from continuing post-acquisition, the acquiring entity should have a robust, fully-documented due diligence and remediation plan, involving both pre- and post-acquisition steps. Failure to have such a plan can expose the company to extensive liability for the continuing misconduct (see, for example, *SEC Press Release, SEC Charges Goodyear With FCPA Violations (Feb. 24, 2015)*, available at *sec.gov*). In particular, the acquiring entity should:

- Conduct a written risk assessment of the target company.
- Perform a forensic audit of the target company's books and records.
- Identify and discipline individuals involved in prior misconduct.
- Identify and review the target company's third-party partners and their contracts, to assess whether to terminate any existing contracts or amend them by including anti-corruption certifications, representations and warranties.
- Ensure that any new contracts with the target company's third-party partners include anti-corruption certifications, representations and warranties.
- Consider implementing a new FCPA compliance program, with an aggressive action timetable.
- Best practices to reach the most favorable outcome for the company.

In addition to these considerations, whether the company has run a thorough and honest internal investigation (see above *Conducting an Internal Investigation*), presented the facts fairly and reacted adequately will be crucial in defending allegations of wrongdoing and reaching the best possible resolution.

POTENTIAL RESOLUTIONS

The range of potential resolutions to an FCPA enforcement action include:

- A monetary settlement with the DOJ or SEC, or both. The settlements often are conditioned on the company's agreement to implement anti-corruption measures and accept a compliance monitor.
- Imposition of a penalty and an injunction, following a civil or an administrative action.
- A civil or criminal complaint brought against the company and any relevant individuals.
- A plea agreement with the DOJ, which is typically used when an individual defendant admits guilt. The agreement may recommend a sentence or fine.

- A deferred prosecution agreement (DPA) with the DOJ, in which the government requests that prosecution of the FCPA claim be deferred to allow the company to cooperate with the government and fulfill the terms of the DPA, which usually include the implementation of anti-corruption measures and often a compliance monitor.
- A non-prosecution agreement (NPA) with the DOJ or SEC, in which the government agrees to refrain from pursuing an enforcement action provided that the company complies with certain conditions for a period of time (usually several years).
- A declination, which is when the government declines to bring an enforcement action.

(See *DOJ and SEC, A Resource Guide to the U.S. Foreign Corrupt Practices Act, at 74-77 (Nov. 14, 2012)*, available at *sec.gov*.)

COOPERATION

The DOJ and SEC may award cooperation credit and provide leniency if a company self-reports an FCPA violation to the government and provides relevant information in a timely manner. Among other benefits, self-reporting and cooperation may lead to reduced charges and fines, an NPA or a DPA.

For example, Ralph Lauren Corp. received notable praise from the government for its self-reporting and extensive cooperation in connection with bribes paid by a subsidiary to Argentinean government officials. The company became aware of the FCPA violation during an internal investigation and timely reported the misconduct to the SEC. The SEC decided not to bring charges, due to the company's "prompt reporting of the violations on its own initiative, the completeness of the information it provided, and its extensive, thorough, and real-time cooperation with the SEC's investigation." (See *SEC Press Release, SEC Announces Non-Prosecution Agreement With Ralph Lauren Corporation Involving FCPA Misconduct (Apr. 22, 2013)*, available at *sec.gov*.)

COMPLIANCE EXPERTS

The government often requires companies to retain an independent compliance monitor as part of a settlement. Because compliance monitors generally are regarded as expensive, intrusive and disruptive to normal business operations, the government has experimented with options short of full compliance monitors, such as compliance consultants or self-reporting requirements.

Regardless of the exact form the compliance expert takes, the company should do its best to help the government select an appropriate person. The compliance expert and his team will become an integral part of the company's operations, possibly for years, and the importance of their ability to work collaboratively with the company's staff cannot be overstated. In developing a short list of candidates to provide to the government, the company should:

- Conduct thorough due diligence.
- Speak with the compliance expert's former clients.
- Interview potential candidates.

The company should seek an expert who recognizes their discrete role and whose ultimate goal is to develop practical and successful compliance improvements, rather than to prove to the government how harsh a critic they can be.

BEST PRACTICES

While the penalty the government ultimately imposes may be out of counsel's hands, careful and strategic lawyering can help steer the government toward a better resolution for the client. For example, counsel can:

- **Designate a "sacrificial subsidiary" to plead guilty.** This would allow the parent company to continue operations and avoid the potentially devastating collateral consequences of a criminal conviction.
- **Negotiate employing a compliance consultant instead of a full compliance monitor.** A compliance consultant's role is intended to be more collaborative, giving the parties room to discuss the ongoing correction of potential issues and avoid direct complaints to the government. Counsel should note that, in some jurisdictions, it is arguably illegal for a US government-mandated compliance monitor with direct reporting lines to the government to oversee a foreign company's compliance program, because it could constitute extraterritorial judicial action. If so, the company may be able to more easily negotiate retaining a compliance consultant in the foreign jurisdiction or arrange for self-reporting, as opposed to a traditional monitor.
- **Consider the collateral consequences of any plea.** Counsel should think carefully about the plea itself as well as the language used in any settlement agreement, as both will have potential consequences for:
  - private actions or foreign proceedings against the company (see below *Follow-on Litigation*);
  - exclusion from government programs (counsel should ensure language is inserted to clarify that any settlement does not constitute a "conviction by final judgment" for bribery-related offenses, as such convictions could cause a company to be excluded from certain EU-administered contracts (see *Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement, Art. 57(1)(b)*));
  - debarment, meaning that the company will be barred from doing business with the government; and
  - cross-debarment by MDBs (see below *MDB Sanctions Proceedings*).

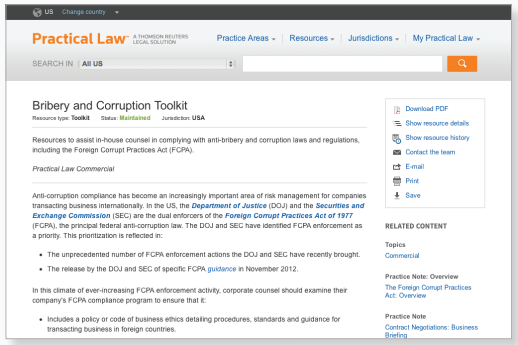
FOLLOW-ON LITIGATION

The FCPA affords no private right of action. However, once an FCPA investigation is announced or a statement of facts filed with a DPA or plea agreement is made public, it is common for third parties to initiate a legal action against the company based on the FCPA-related misconduct. Common types of follow-on litigation include:

BRIBERY AND CORRUPTION TOOLKIT

The Bribery and Corruption Toolkit available on practicallaw.com offers a collection of resources to assist counsel in ensuring company compliance with anti-bribery and corruption laws and regulations. It features a range of continuously maintained resources, including:

- The Foreign Corrupt Practices Act: Overview
- Foreign Corrupt Practices Act Anti-Corruption Policy
- Foreign Corrupt Practices Act Compliance Checklist
- Foreign Corrupt Practices Act (FCPA) Training Hypotheticals for Employees: Presentation Materials
- Developing a CSR Supply Chain Compliance Program
- M&A Due Diligence: Assessing Compliance and Corruption Risk
- Policy for the Use of Third-party Agents Outside of the United States
- Underwriting Agreement: FCPA Representation
- Anti-Corruption Regimes in the UK and US: A Comparison of the UK Bribery Act 2010 and the US Foreign Corrupt Practices Act 1977



- Shareholder actions.
- Claims by foreign governments brought under the Racketeer Influenced and Corrupt Organizations Act (RICO).
- Lawsuits brought by competitors.
- MDB sanctions proceedings.

SHAREHOLDER ACTIONS

In recent years, there have been several shareholder derivative and securities fraud cases filed following FCPA government investigations. These actions typically allege that the company's officers and directors violated their fiduciary duties by not enforcing an adequate compliance program, by ignoring evidence of bribery, or by making false statements about the effectiveness of a company's compliance program or its adherence to all applicable anti-corruption laws. Often, the allegations appear to be pulled straight from filings by the DOJ and SEC. Although many of these cases have been dismissed on pleadings, amended pleadings have been filed and the litigation can be very costly and disruptive for the company. This has resulted in numerous companies choosing ultimately to settle the matters.

One high-profile case involved aluminium producer Alcoa Inc., which faced a derivative suit alleging breaches of fiduciary duty, filed soon after the DOJ initiated an FCPA investigation (see *Box, Notable Recent Settlements*). Alcoa's settlement of the derivative suit included compliance reforms and $3.75 million in attorneys' fees (see *Stipulation of Settlement, Rubery v. Kleinfeld, No. 12-00844 (W.D. Pa. Oct. 10, 2014); Exhibit A to Stipulation of Settlement, Rubery v. Kleinfeld, No. 1200844 (W.D. Pa. Oct. 10, 2014)*).

Search Shareholder Derivative Litigation for more on litigating and settling a shareholder derivative lawsuit.

Shareholders' securities fraud claims often argue that the disclosure of an active FCPA government investigation or a resolution of FCPA charges is evidence that the company knowingly withheld material information regarding internal control failures from its shareholders.

For example, after improper payments by FARO Technologies, Inc. (FARO) became public, shareholders filed an action alleging that the company overstated its sales by including sales achieved through unlawful conduct in Asia in violation of the FCPA. FARO chose to settle the securities fraud claims for $6.875 million, rather than litigate them while battling simultaneous enforcement actions with the DOJ and SEC (see *Final Judgment and Order of Dismissal with Prejudice, In re Faro Techs. Sec. Litig., No. 05-01810 (M.D. Fla. Oct. 3, 2008)*). FARO settled a subsequent derivative lawsuit for $400,000 (see *Order and Final Judgment, Alverson v. Caldwell, No. 08-0045 (M.D. Fla. Apr. 24, 2009)*). Notably, the total settlement of the actions was significantly larger than the $2.95 million FARO paid to settle the FCPA claims brought by the government (see *DOJ Press Release, Faro Technologies Inc. Agrees to Pay $1.1 Million Penalty and Enter Non-Prosecution Agreement for FCPA Violations (June 5, 2008)*, available at *justice.gov*).

However, securities fraud claims based on FCPA violations often do not pass the motion to dismiss stage. Courts have held that a company's generic statements about its compliance with applicable laws are non-actionable puffery and, without more, these statements cannot demonstrate the requisite scienter. Counsel may consider moving to dismiss the fraud-based claims before discussing any settlement, although they also must weigh the actual and reputational costs associated with continued litigation.

In a recent case, for example, the US District Court for the Southern District of New York granted Avon Products Inc.'s motion to dismiss, rejecting, among other things, the shareholders' claim that a public statement regarding the strength of Avon's ethics policy was an actionable statement (see *Memorandum Opinion and Order, City of Brockton Ret. Sys.*

v. Avon Prods. Inc., No. 11-4665 (S.D.N.Y. Sept. 29, 2014)). The plaintiffs subsequently filed a second amended complaint, and Avon's motion to dismiss the second amended complaint is pending. However, the parties have indicated to the court that they will hold mediation sessions in April and May 2015 to try to resolve the pending claims (see *Letter addressed to Judge Paul G. Gardephe from Peter C. Hein dated 2/18/2015 re: Status Update, No. 11-4665 (S.D.N.Y. Feb. 18, 2015)*).

Search The Rise and Reformation of Private Securities Litigation for more on securities fraud actions.

FOREIGN GOVERNMENT RICO CLAIMS

Foreign governments, state-controlled companies and private entities also have sought to recoup damages through RICO claims against companies that made corrupt payments to government officials. These suits often are filed soon after the DOJ or SEC announces an FCPA enforcement action.

For example, in late 2014, Mexican state-owned oil company Petróleos Mexicanos (PEMEX) filed suit against Hewlett-Packard (HP), claiming RICO and other violations, following HP's resolution of criminal and civil charges with the DOJ and SEC for activities linked to PEMEX officials (see *Complaint, Petróleos Mexicanos v. Hewlett-Packard Co., No. 14-05292 (N.D. Cal. Dec. 2, 2014)*). A motion to dismiss is pending in the case (see *Defendants' Corrected Notice of Motion and Motion to Dismiss Complaint, No. 14-05292 (N.D. Cal. Feb. 10, 2015)*).

Similarly, the Republic of Iraq filed RICO and other claims against several companies for bribery-related losses following the DOJ's and SEC's broad investigations of corrupt payments involving Iraq's oil-for-food program. The district court dismissed the claims and the US Court of Appeals for the Second Circuit affirmed the dismissal, holding in part that the *in pari delicto* defense, which bars liability when the plaintiff is equally at fault, is available in RICO cases (see *The Republic of Iraq v. ABB AG, 768 F.3d 145, 163 (2d Cir. 2014)*).

COMPETITOR LAWSUITS

Competitors who allegedly lost business opportunities due to a company's bribery of foreign officials are now using a mix of RICO, antitrust and state unfair business practices laws to seek damages.

For example, in 2008, Supreme Fuels Trading FZE (Supreme), a United Arab Emirates-based company, sued Florida-based International Oil Trading Company Co. (IOTC) and its foreign affiliates for damages it allegedly suffered due to IOTC's bribery of Jordanian officials to obtain the sole authorization to transport fuel through Jordan into Iraq. Basing its claims on RICO, the Clayton Act, the Sherman Act, and various Florida state antitrust and trade practices laws, Supreme alleged that IOTC's bribery prevented Supreme and others from bidding on US government contracts. In February 2011, the parties settled the lawsuit, with IOTC agreeing to pay $5 million in damages (see *Order Granting Plaintiff's Motion to Enforce Settlement, Supreme Fuels Trading FZE v. Sargeant, No. 08-81215 (S.D. Fla. Feb. 3, 2011)*).

MDB SANCTIONS PROCEEDINGS

Financial institutions formed by a group of countries to provide financing for development work (such as large infrastructure projects), so-called MDBs, are increasingly initiating investigations of companies accused of corruption in connection with MDB-financed projects. While MDBs are not allowed to impose sanctions based solely on a national court's ruling or an investigative agency's findings, as a practical matter, an MDB's findings often reference the same fact patterns as those in related FCPA prosecutions by the DOJ and SEC. The statement of facts filed publicly with a DPA or plea agreement serves as a ready-made starting point for an MDB's sanctions inquiry.

Based on their findings, MDBs may offer various resolutions and impose a range of penalties, including:

- Letters of reprimand.
- Negotiated resolution agreements (NRAs), which are similar to DPAs and can come with:
  - large settlement amounts; and
  - compliance program requirements.

  For example, in 2009, as part of its bribery-related NRA, Siemens AG paid the World Bank $100 million and was required to hire a compliance monitor (see *World Bank, Stolen Asset Recovery Initiative, Siemens AG (World Bank Settlement)*, available at *star.worldbank.org*).
- Debarment decisions and cross-debarment agreements, under which a debarment decision against a company by one MDB is enforced by other MDBs through a formal agreement (see *Agreement for Mutual Enforcement of Debarment Decisions (Apr. 9, 2010)*, available at *ebrd.com*). Organizations that are not part of the agreement also may choose to exclude debarred parties automatically. Because this can be enterprise-threatening, it is crucial for companies under investigation by an MDB to negotiate a resolution short of debarment, or find a sacrificial subsidiary (see above *Best Practices*).