Advisory

JANUARY 2016

*If you have any questions about this Advisory, please contact:*

JOSEPH MARTINI
203.363.7603
jmartini@wiggin.com

MICHAEL MCGINLEY
203.363.7638
mmcginley@wiggin.com

# Foreign Corrupt Practices Act Enforcement 2016: In Like a Lamb, Out Like a Lion

By Joseph W. Martini and Michael T. McGinley*

*The Foreign Corrupt Practices Act ("FCPA") prohibits companies and individuals with sufficient ties to the United States from engaging in international bribery for the purpose of obtaining or retaining business. The U.S. Government has taken steps recently to increase the effectiveness of its FCPA enforcement. Companies with U.S. ties should be familiar with the law and ensure their internal compliance programs are commensurate with their FCPA exposure.*

## INTRODUCTION

In 2015, the U.S. Government significantly bolstered its resources dedicated to combat international corporate bribery under the Foreign Corrupt Practices Act ("FCPA"). By announcing the addition of a team of FCPA-dedicated prosecutors, plus three new squads of investigators and the use of a data-driven, crime-prediction approach, the Government doubled down on its effort to root out international corporate corruption. This year, those resources will be tested as the Government seeks to show return on its investment.

The FCPA, jointly enforced by the United States Department of Justice ("DoJ") and Securities and Exchange Commission ("SEC"), prohibits bribery of foreign government officials for the purpose of obtaining or retaining business. The FCPA is applicable to U.S. citizens and entities and foreign companies with certain ties to the United States. In addition, the Government views its jurisdiction over non-U.S. companies and individuals expansively. Foreign companies and individuals who do not themselves violate the FCPA may still be convicted of conspiring with a domestic entity to violate the FCPA—even if the foreign company or individual did not act in furtherance of the violation while in the United States.

Both the DoJ and SEC have signaled that 2016 will be an active year for FCPA enforcement actions. Below are five observations for what 2016 may hold in store, and what you can do now to be ready.

## IN LIKE A LAMB, OUT LIKE A LION

*Expect an uptick in FCPA activity.* The last year was notable for the slowdown in FCPA enforcement activity. Expect a change in 2016. In November 2015, Leslie Caldwell, Assistant U.S. Attorney of DoJ's Criminal Division, announced that DoJ was "increasing attention to the investigation and prosecution of international corruption under the FCPA." To that end, Caldwell announced DoJ is adding 10 new prosecutors to the Fraud Section's FCPA Unit. This hiring spree follows an earlier announcement that the Federal Bureau of Investigation was tripling the number of agents focused on overseas bribery. Caldwell noted that these additions align DoJ's resources and FCPA ambitions for the first time.

CONTINUED ON NEXT PAGE

Foreign Corrupt Practices Act Enforcement 2016: In Like a Lamb, Out Like a Lion

While these additional resources give the Government a tremendous boost to its FCPA enforcement power, it will be pressed to show these resources are being used effectively. Similarly, the SEC has signaled its intent to pursue FCPA violations aggressively, and the existence of several not-yet-public investigations appears likely. Accordingly, this year we expect a rise in the number of FCPA enforcement matters made public and a more significant uptick in the value of settlements.

## EXECUTIVES IN THE CROSSHAIRS

*Expect the DoJ and the SEC to step up their attempts to hold individual executives accountable.* On September 10, 2015, Deputy Attorney General Sally Quillian Yates unveiled DoJ's new corporate fraud enforcement policy. Her speech articulated DoJ's aggressive new attempt to tackle corporate fraud by focusing on individual accountability. Yates spoke bluntly, noting that "nothing discourages criminal behavior like prison." Yates emphasized that a company must disclose completely all facts relevant to individual misconduct before the company would be eligible to receive any credit for cooperation. Yates highlighted that this is "a substantial shift from prior practice," and said that if a company under investigation did not cooperate 100% with DoJ, the company would receive absolutely no credit.

Yates acknowledged that this policy shift is not without risk to the Government. She said that individuals may be more likely to choose to go to trial, and that corporations might decide under this new calculus that it is no longer in their interests to cooperate with the Government. Yates did not appear concerned, stating, "Only time will tell, but if that's what happens, so be it."

While Yates was discussing DoJ's approach to corporate fraud generally and not specifically in the context of an FCPA enforcement matter, Ms. Caldwell's speech two months later made clear that the policy Yates articulated applies to FCPA enforcement, and that "companies seeking credit must affirmatively work to identify and discover relevant information about the individuals involved through independent, thorough investigations." Caldwell also noted that internal FCPA investigations "cannot end with a conclusion of corporate liability, while stopping short of identifying those who committed the underlying conduct."

The SEC has espoused a similar approach and brought FCPA cases against individuals over 20% of the time in 2015. Andrew Ceresney, Director of the Commission's Division of Enforcement, announced in November 2015 that "the Commission is committed to holding individuals accountable, and I expect you will continue to see more cases against individuals." At the same time, Ceresney admitted that FCPA cases present the Commission with "formidable challenges to establishing individual liability," including the difficulty in establishing personal jurisdiction over foreign nationals living outside the United States as well as evidentiary challenges and expenses that arise from overseas witnesses and documents.

In sum, while Government pursuit of individuals under the FCPA is not a new policy, expect the Government to place additional pressure on companies at the onset of investigations to identify and provide information about employees with potential culpability and for the Government to predicate any credit on a company's total cooperation.

## SELF-REPORTING HAS SIGNIFICANT UPSIDE, BUT IS NOT WITHOUT RISK

*Expect increased Government pressure on companies to self-report.* Self-reporting is a "bet-the-company" strategic decision and should be considered with great care. The Government wants companies to self-report, for obvious reasons, not the least of which is the fact that overseas-based bribery schemes are difficult to detect and prosecute. Deciding to self-report an FCPA violation offers a company significant benefits and is often a wise decision, but doing so creates a certain and immediate legal exposure and accompanying costs that must be evaluated.

According to the SEC's Ceresney, "self-reporting is critical to the success of SEC's cooperation program." Caldwell defined self-disclosure as the disclosure of "all relevant facts about the individuals involved in the conduct" within a "reasonably prompt time" after a company becomes aware of an FCPA violation. A company that decides to self-report should not expect to receive full credit automatically, however. According to DoJ's Caldwell, "a company that wishes to be eligible for the maximum mitigation credit in an FCPA case must do three things: (1) voluntarily self-disclose; (2) fully cooperate; and (3) timely and appropriately remediate."

Both the DoJ and SEC claim that self-reporting and cooperating results in tangible benefits to companies. These benefits

CONTINUED ON NEXT PAGE

include reduced charges and penalties, deferred prosecution agreements (DPAs) and non-prosecution agreements (NPAs), and, in certain instances involving minimal violations, no charges. To illustrate, Caldwell distinguished DoJ's handling of two FCPA cases. The first involved French power company Alstom S.A. According to Caldwell, Alstom did not voluntarily disclose its misconduct and refused to cooperate with DoJ's investigation for several years. Alstom ultimately admitted to its criminal conduct and agreed to pay a penalty of $772 million.

In contrast, PetroTiger self-disclosed that its employees had engaged in a scheme to win a $39 million oil-services contract by bribing Colombian officials. After self-disclosing its conduct, PetroTiger fully cooperated in the ensuing investigation, and DoJ declined to prosecute the company. Likewise last year, according to the SEC's Ceresney, the Commission gave companies significant credit for cooperation in over a half dozen cases—to include reduced penalties at a fraction of respective disgorgement amounts and a DPA. In addition, last year witnessed the first case in which the Commission decided not to seek a civil penalty against a company despite requiring them to pay disgorgement. The settlement, which involved Goodyear Tire & Rubber Company, was significant because, while Goodyear agreed to pay a $16 million disgorgement and interest to settle the matter, without the company's significant cooperation, the civil penalty could have been substantial. Take, for example, the SEC's 2015 settlement with BHP Billiton—BHP Billiton did not self-report and was slapped with a $25 million civil penalty.

The SEC has taken additional action in an effort to incentivize companies to self-report and cooperate with the Commission. Ceresney explained one way the Commission is incentivizing companies: "The Enforcement Division has determined that going forward, a company must self-report misconduct in order to be eligible for the Division to recommend a DPA or NPA to the Commission in an FCPA case."

The Government wants you to self-disclose—but should you? Although there are exceptions, companies generally are not required to self-disclose criminal wrongdoing. In fact, according to the DoJ, most FCPA cases it brings are investigated and prosecuted without self-disclosure. New incentives for whistleblowers to report compliance violations, however, coupled with the increasing role of social media to publicize the grievances of disgruntled employees and the observations of competitors make a decision not to self-report a risky one. Says Ceresney, "Companies are gambling if they fail to self-report FCPA misconduct to us." Still, self-reporting is a significant decision and should be undertaken only after careful discussion with legal counsel and compliance personnel.

## BIG DATA ANALYTICS PUTS THE U.S. GOVERNMENT AT YOUR DOORSTEP, ANYWHERE IN THE WORLD

*Expect more focused Government scrutiny where corporate activity occurs in geographic locations with high levels of corruption.* Your geographically dispersed operating locations may subject you to increased scrutiny thanks to the Government's use of big-data analytics. Using sophisticated, data-driven analytic tools, the U.S. Government is able to identify crime patterns around the world with increasing precision, allowing it to employ its resources in geographic areas historically likely to be at higher risk of fraud. Andrew Weissmann, DoJ's Fraud Section Chief, recently noted that DoJ is using a COMPSTAT approach popularized by the New York Police Department to identify and predict areas of high corruption. Said Weissmann, "if you are operating [in an area with statistically high levels of corruption], and are not taking appropriate precautions to detect and deter FCPA violations, you won't receive a soft shoulder at the Fraud Section. Vigilance will be expected when operating in such areas." Although Weissmann did not describe the specific technology DoJ is using for its analysis, what this means is that the Government has an improved ability to predict where bribery will occur and apply its resources accordingly.
Weissmann's warning should enter into the strategic calculus of businesses deciding if, when, or how to operate in a high-risk area. For a company operating in a high-risk area already, the question becomes whether the company has established a compliance program with monitoring and auditing functions commensurate with the risk level.

## CAN YOUR COMPLIANCE POLICY WITHSTAND HEIGHTENED SCRUTINY?

*Expect increased Government scrutiny on your compliance program's policies and execution.* Companies should take the time necessary to ensure their compliance policies are "thoughtfully designed and sufficiently resourced." Compliance policies do not exist in a vacuum. Rather, they are creations of the experiences and judgment of a company's executives and account

CONTINUED ON NEXT PAGE

## Foreign Corrupt Practices Act Enforcement 2016: In Like a Lamb, Out Like a Lion

for the company's business outlook and prevailing industry standards. As such, compliance policies are complex tools. DoJ acknowledged as much by recently hiring an experienced compliance counsel, Hui Chen, to support the work of its FCPA prosecutors. Chen will assist prosecutors to develop benchmarks to evaluate corporate compliance and remediation measures. According to Caldwell, Chen will advise prosecutors on whether a company's compliance policy was "thoughtfully designed and sufficiently resourced" to address the company's FCPA risks.

Thoughtfully designed and sufficiently resourced compliance programs have several characteristics, which Caldwell spelled out in a speech in May of last year. Specifically, they:

- start with the consistent and visible backing of senior leadership;
- are run by senior executives with unfettered access to the company's internal auditors and Board of Directors;
- extend beyond the company's formal policies and into emails and other records that demonstrate to the Government that the company effectively conveyed a culture of compliance, even when contrary to profits;
- are funded adequately;
- have an established process for investigating and documenting allegations of violations;
- are kept current and updated to reflect changes resulting from mergers, acquisitions, or changes in corporate structure;
- contain an effective and confidential internal system for reporting compliance violations;
- contain procedures designed to hold employees accountable and to reward compliant conduct; and
- contain procedures for terminating business relationships with third parties (e.g., vendors, agents, or consultants) who violate laws or policies.

An effective compliance program should contain both audit and monitoring components. An effective audit function periodically evaluates a company's internal controls and provides feedback directly to senior management, with auditors enjoying direct access to the audit committee and Board of Directors. By contrast, an effective monitoring program functions as part of a company's daily operations and allows a company to determine in real-time if its internal controls are operating sufficiently. When designed correctly and given adequate resources, these components provide companies the ability to prevent, detect, and respond to compliance issues before the Government comes knocking.



**Joseph Martini is a partner of Wiggin and Dana LLP, and Chair of Wiggin and Dana's White Collar Defense, Investigations, and Corporate Compliance Group. Wiggin and Dana has offices in Connecticut, New York, Philadelphia and Washington.D.C. Michael McGinley is an associate in the Corporate and Litigation Groups in Wiggin and Dana's Stamford, Connecticut office. Mr. Martini can be contacted at jmartini@wiggin.com. Mr. McGinley can be contacted at mmcginley@wiggin.com.*