New York Law Journal
Compliance
An ALM Publication
WWW.NYLJ.COM
MONDAY, NOVEMBER 7, 2011

Tuma/MCT

FCPA Violations In the **Whistleblower Era**

BY MARK S. COHEN, JONATHAN S. ABERNETHY AND S. GALE DICK

THE NEWLY-IMPLEMENTED whistleblower provisions of the Dodd–Frank Wall Street Reform and Consumer Protection Act, which provide for bounties for tips reported to the U.S. Securities and Exchange Commission (SEC) about securities violations, have already produced a wave of Foreign Corrupt Practices Act (FCPA) whistleblowers. FCPA violations are included within the violations for which a whistleblower may be eligible to obtain an award.[1] Since Dodd-Frank was passed in July 2010, the SEC has received approximately one FCPA-related whistleblower tip per day.[2] This pace can be expected to accelerate, particularly as the SEC builds the infrastructure to leverage such tips into more aggressive and effective enforcement. The SEC's newly-opened Whistleblower Office and a $452 million Investor Protection Fund to pay awards—not to mention a prominent link on the SEC website to all of the forms a prospective whistleblower needs to report a tip and qualify for an award—have brought the whistleblower provisions fully to life.

The significant amount of activity generated by the whistleblower program in the FCPA context is no surprise. Under Dodd-Frank, whistleblowers can be

MARK S. COHEN *is a partner and co-founder, and* JONATHAN S. ABERNETHY *is counsel, at Cohen & Gresser. Both are former Assistant U.S. Attorneys.* S. GALE DICK *is an associate at the firm.*

awarded between 10 and 30 percent of monetary sanctions obtained by the SEC and criminal authorities in a related action, assuming the whistleblower's information leads to an enforcement action with more than $1 million in fines.

These incentives have coincided with a spike in FCPA enforcement. In the last three years, the SEC and the Department of Justice's aggressive FCPA enforcement has led to eight corporate settlements with more than $100 million in combined civil and criminal fines. Five of these settlements had fines in excess of $300 million.[3] Payments to FCPA whistleblowers in the future, therefore, could easily be in the tens of millions of dollars.

For in-house FCPA lawyers, corporate compliance officers, and outside advisers, the whistleblower program presents a new challenge. Many corporations subject to the FCPA have implemented compliance programs carefully designed to promote internal reporting. Such programs offer many advantages, including early detection and prevention of FCPA violations and, perhaps most importantly, the ability to self-report violations to regulators. In issuing Final Rules for the whistleblower program, however, the SEC did not require whistleblowers to report their allegations internally through existing corporate compliance programs. Thus, multinational companies now face risks that a disgruntled employee or former employee will go straight to the SEC with an FCPA tip before informing anyone in the company's compliance or legal department.

One possible outcome is that highly developed FCPA compliance programs that rely on internal reporting may be circumvented. Even more serious, when an FCPA whistleblower reports a tip to the SEC and the matter results in an enforcement action or a criminal case, the company in question likely will not be eligible for a reduced fine under the federal Sentencing Guidelines for voluntarily disclosing the potential FCPA problem.[4]

No company can eliminate the risk of an employee or former employee giving an FCPA tip to the SEC. But companies can take steps within their existing compliance mechanisms to increase the odds that a would-be whistleblower will alert the company to the problem before telling the SEC.

This article begins with a review of key provisions of the whistleblower rules, and then proposes a number of ways companies might strengthen their FCPA compliance programs in this new era of the FCPA whistleblower.

The Whistleblower Rules

The whistleblower rules require the SEC to award at least 10 percent and no more than 30 percent of total monetary sanctions to a whistleblower who voluntarily provides the SEC with original information that leads to successful enforcement action with more than $1 million in penalties.[5] "Original information" is defined as information that is derived from a whistleblower's independent knowledge or analysis and that is not already known to the SEC nor exclusively derived from the media, a judicial or administrative hearing, or a government report.

The whistleblower rules require the SEC to award between **10 and 30 percent** of total monetary sanctions to a whistleblower who voluntarily provides the SEC with **original information** that leads to successful enforcement action with more than $1 million in penalties.

A whistleblower need not have first-hand knowledge of a potential violation to qualify, however; "independent knowledge" may be gained from "experiences, communications and observations" with others inside or outside of a company. Information obtained from a communication subject to the attorney-client privilege is excluded from the definition of original information.[6] In addition, certain categories of employees, including compliance, audit, and legal personnel who obtain information about a potential violation, are generally excluded from obtaining awards.[7]

To be considered "information that leads to a successful enforcement action," the whistleblower's information must be "sufficiently specific, credible, and timely" to cause the SEC to commence an investigation and bring a successful action based in whole or in part on the information. Whistleblowers also may qualify if they give the SEC information about conduct that the SEC is already investigating, and that information "significantly contributed" to the success of the action.[8]

The whistleblower rules also contain a "lookback provision" for whistleblowers who initially report information pursuant to a company's internal compliance procedures. If the whistleblower submits the same information to the SEC within 120 days of notifying the company, then the whistleblower will be deemed to have provided the information to the SEC on the date he or she first notified the company.[9] This rule protects the original whistleblower if, during this 120-day period, another whistleblower tips the SEC to the same conduct, provided that the first whistleblower's information was specific and credible. The SEC emphasized that this lookback provision is designed to support compliance programs "by allowing employees to take their concerns about possible

violations to appropriate company officials first while still preserving their rights under the Commission's whistleblower program."[10]

In another gesture of intended support for existing internal compliance programs, the whistleblower rules provide that a factor that may increase the amount of an award is "whether, and the extent to which, the whistleblower… participated in internal compliance systems."[11] Conversely, if a whistleblower interfered with those systems "to prevent or delay detection," or if a whistleblower made a false statement "that hindered an entity's efforts to detect, investigate, or remediate the reported securities violations," the award likely will be reduced.[12]

The Dodd-Frank Act also contains an anti-retaliation provision that prohibits an employer from discharging, demoting, or suspending a whistleblower because of the whistleblower's lawful act of bringing a tip to the SEC's attention. Whistleblowers may bring actions in federal court to enforce this provision and may be entitled to reinstatement at the same seniority level, two times the value of any back-pay with interest, and attorney's fees.[13]

Bolstering FCPA Compliance

Companies should consider several steps to encourage employees or former employees to first report potential FCPA violations internally, before going to the SEC.

Employee Certifications. As part of their FCPA compliance program, companies often require employees to certify on an annual basis that they are unaware of any foreign bribery or accounting and internal controls violations. If the employee is aware of a potential violation, the certification form asks the employee to describe the conduct in question.

Companies, particularly those with operations in regions of the world that are known to have a high risk of corruption,[14] should consider augmenting their certification process in at least a few different respects. First, it may be wise to require employees to certify every quarter or every six months rather than annually. More frequent certifications will increase the odds that a company will learn about potential FCPA violations earlier and be better able to address them. This more timely information flow, in turn, will allow companies to investigate foreign bribery issues proactively rather than simply reacting to an SEC request for information about a whistleblower complaint that may ultimately prove meritless.

The whistleblower rules also contain a **"lookback provision"** for whistleblowers who **initially report** information pursuant to a company's **internal compliance procedures**.

Second, periodic certification forms should be made as user-friendly and as detailed as possible. In foreign language countries, they should be printed in the local language(s). In addition, rather than simply asking employees to describe in their own words conduct that could have violated the FCPA, companies may want to include in the certification forms examples of conduct that might constitute corruption "red flags" and ask employees to check boxes if they have noticed such conduct occurring. Employees who are forced to answer specific questions (and certify the truthfulness of their responses) will be less likely to make false statements, which under the whistleblower rules would be grounds for reducing their award.

Third, departing employees should be asked to fill out a certification form asking if they are aware of any conduct in their tenure with the company that might have violated the FCPA. Because whistleblowers are often disgruntled *former* employees, companies should have departing employees "go on record" about any FCPA red flags they may have seen.

Training. Regular employee training is a staple of well-developed FCPA compliance programs, and for good reason: it tends to work. While the methods vary, such training often is a combination of in-person sessions for new employees paired with the requirement that employees periodically view a video FCPA training course on their computers.

Naturally, video courses have the advantage of training large numbers of employees in a cost-effective manner. But companies should consider conducting more frequent in-person training in light of the risks imposed by the whistleblower provisions. In the end, nothing encourages internal reporting more effectively than when companies show they care about compliance with the FCPA and take allegations of wrongdoing seriously. In-person training is one way to showcase this commitment to compliance.

In addition to doing more in-person training, companies should consider updating the content of the training. A section should be included on how the company receives and investigates FCPA allegations, and how employee confidentiality is paramount. The message is that if an employee reports a potential FCPA violation to the compliance or legal department, his or her report will be taken seriously, investigated, and dealt with appropriately. Employees should also be reminded that they owe fiduciary duties to their employers and that part of those duties include reporting potential

violations. The FCPA compliance policies of many companies require employees to report potential violations internally, and training should remind employees of this requirement. Inclusion of these points in FCPA training will serve as a reminder that employees should always raise their concerns with compliance and/or legal personnel.

Risk Assessments, Audits and Internal Investigations. Multinational companies with well-developed FCPA compliance programs periodically conduct formal assessments of corruption risks in high-risk regions, or audits of the compliance program itself to test its effectiveness. Company personnel who conduct these assessments or audits might target for interviews key employees who interact with officials of foreign governments in such areas as licensing, permitting, or other required governmental approval processes. These interviews might not be subject to the attorney-client privilege, and therefore information gleaned from them could constitute "original information" under the whistleblower rules.

In conducting these interviews, a company must be mindful of the way in which questions are worded so as to not *create* whistleblowers and short-circuit the company's own process. If an interviewee becomes aware of a potential FCPA issue from the interview, and combines that information with his or her own investigation and analysis, he or she could develop a tip that is sufficiently specific and credible to gain the attention of the SEC's Whistleblower Office. Accordingly, company personnel who conduct these audits should exercise the utmost discretion and ask open-ended questions that do not reveal any information that could form the basis for a tip.

The same is true of internal investigations. Such investigations are typically conducted pursuant to the attorney-client privilege, and therefore information conveyed in outside counsel's interview of an employee would not be "original information." Nevertheless, there is a risk that an interviewee will convey information gained in the interview to a colleague. Since the conversation between these two employees is not privileged, the employee receiving the information could use it along with other analysis to develop a tip that is based on "original information."

Anonymous Internal Reporting: That the whistleblower rules do not require internal reporting as a precondition to payment of a bounty obviously does not mean that internal reporting programs can be neglected. On the contrary, companies that have not already established dependable, anonymous channels for employees to report suspected violations should do so right away. Those that have such programs in place should review and, where necessary, enhance them. The programs should be transparent and widely publicized, with ironclad protections against retaliation.

Conclusion

The silver lining for companies that adapt their compliance programs to the reality of the whistleblower provisions is that doing so could further some of the goals for which such compliance goals were originally designed, namely, the effective prevention and detection of FCPA violations. Similarly, robust FCPA compliance programs can reduce the severity of any penalties imposed by regulators.[15] Adapting compliance programs to the challenge posed by new whistleblower rules can only help in this regard. Although this process will no doubt incur additional compliance costs for multinationals, when compared to the far greater costs of dealing with an SEC investigation initiated by a whistleblower complaint, this will be money well-spent.

1. The FCPA prohibits corrupt payments or offers to pay money or anything of value to foreign government officials or third parties acting on their behalf, when such payments or offers to pay are made to assist in obtaining new business or retaining existing business. The FCPA also contains an accounting and internal controls provision that, in essence, requires U.S. public companies and foreign companies listed on U.S. stock exchanges to maintain accurate books and records and to have sound internal controls.
2. "After Dodd-Frank, SEC Getting at Least One FCPA Tip a Day," Corruption Currents Blog, Wall Street Journal, Sept. 20, 2010.
3. The FCPA Blog, "Top 10 FCPA Enforcement Actions," last published April 8, 2011, available at http://www.fcpablog.com/blog/2011/4/8/jj-joins-new-top-ten.html.
4. See U.S.S.G. §8C2.5(g)(1) (corporation can obtain a reduced fine if, "*prior to an imminent threat of disclosure or government investigation,*" it self-reports an offense to "appropriate governmental authorities," cooperates in the investigation, and accepts responsibility for its conduct) (emphasis added).
5. 17 C.F.R. §240.21F-3.
6. 17 C.F.R. §240.21F-4(b).
7. Id.
8. 17 C.F.R. §240.21F-4(c).
9. 17 C.F.R. §240.21F-4(c)(3).
10. SEC Release No. 34-64545, Implementation of the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934, May 25, 2011, at 91.
11. 17 CFR 240.21F-6(a)(4).
12. 17 CFR 240.21F-6(b)(3).
13. 15 U.S.C. §78u-6(h)(1).
14. See Transparency International's yearly Corruption Perceptions Index (CPI), available at http://www.transparency.org/policy_research/surveys_indices/cpi/2010/results. The CPI measures perceived levels of corruption around the world.
15. See U.S.S.G. §8C2.5(f)(1) (providing for a reduced fine if a corporation "had in place at the time of the offense an effective compliance and ethics program").

Reprinted with permission from the November 8, 2011 edition of the NEW YORK LAW JOURNAL © 2011 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-11-11-12

COHEN & GRESSER LLP
800 Third Avenue
New York, NY 10022
Ph 212 957 7600
Fax 212 957 4514
www.cohengresser.com