BNA

White Collar Crime Report

VOL. 6, NO. 15 JULY 29, 2011

WHISTLEBLOWERS

The SEC Releases Whistleblower Bounty Rules—So Now What?

BY T. MARKUS FUNK AND ASSAD H. CLARK

''Focus on marketing. Market what [your compliance] program means, what it doesn't mean. . . . [M]ake your program more robust, more transparent, and make it clear that, when people come to the internal compliance function and identify wrongdoing that wrongdoing is remediated and that individual is not punished for coming forward. . . . If you are setting the tone at the top, you want your employees to come to you first. . . . Make your compliance programs [as] up to speed and robust as possible [and] market, market, market, that would be my strongest advice.''—Sean McKessy, chief of the SEC's Office of the Whistleblower, June 15, 2011.

Practitioners in the exploding field of corporate anti-corruption compliance need little convincing that today we find ourselves in what Assistant Attorney General Lanny Breuer aptly characterized as ''a new age of [significantly ramped-up U.S. and foreign anti-corruption] enforcement.''[1] This article will discuss how the SEC's much-anticipated May 25 whistleblower rules fall within this enforcement paradigm, and will examine how the rules operate to put a premium on ensuring that a covered[2] company's compliance efforts

[1] *See generally*, T. Markus Funk, *Another Landmark Year: 2010 FCPA Year-In-Review and Enforcement Trends For 2011*, BLOOMBERG LAW REPORTS (Jan. 3, 2010).

[2] The public/private company distinction warrants further clarification. Following the SEC's issuance of its new rules, many U.S. and foreign law firms sent out client alerts and updates, often including variants of the following: ''The Rules,

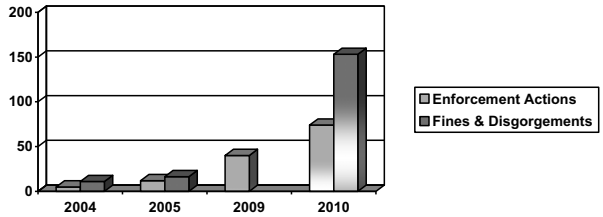
 ISSN 1559-3185

are *effective* and *user-friendly*, rather than merely present. Such critical self-appraisal must be front and center because, despite the vigorous objections from the business community, the new rules allow tipsters to bypass company internal reporting mechanisms and go directly to the SEC to blow the whistle on allegedly corrupt conduct. This makes it more critical than ever for companies to create incentives motivating potential employee whistleblowers to report perceived problems internally first.

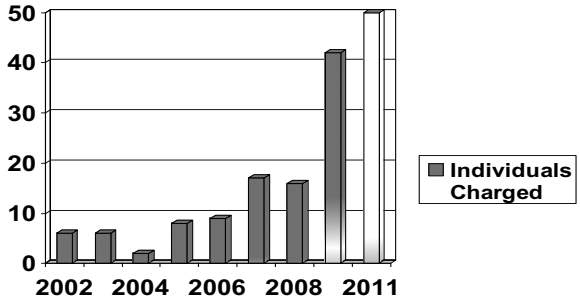
The New Era Of Anti-Corruption Enforcment Is Indeed Upon Us

Those who run afoul of U.S. and foreign anti-corruption laws face an unprecedented array of severe sanctions, including corporate and individual civil and criminal penalties, potential debarment from federal contracts,[3] license terminations, shareholder lawsuits, adverse publicity, and reputational damage.

The available statistics underscore that the U.S. government means business when it comes to anti-corruption enforcement.



As noted below, one of the hallmarks of the government's ''new age of enforcement'' is its re-dedicated efforts to prosecute individuals involved in acts of alleged corruption. In fact, never before have company officers and employees, as well as transaction partners and middlemen,[4] been more exposed to the very real threat of imprisonment and criminal and civil sanctions resulting from their involvement in a company's corrupt conduct.



So why has the government sprung into action so (relatively) quickly, and what are the reasons for believing that this trend in vigorous enforcement will continue? The key developments are:

- expanding multi-jurisdictional law enforcement cooperation;
- increasingly proactive and aggressive investigative approaches and techniques that treat incidences of corporate corruption like ''street crimes'' (*i.e.*, employing wiretaps, cooperators, undercover officers, etc.);
- a new focus on prosecutions of individuals, including bribe recipients and middlemen;
- executive branch pressure to deliver successful prosecutions;
- industry-specific enforcement efforts;
- law enforcement specialization; and
- increased rates of voluntary disclosures by companies and individuals.

Despite a slow start, 2011 is shaping up to be another banner year in civil penalties stemming from FCPA violations. Companies resolving criminal and civil FCPA charges this year include Tyson Foods Inc., Ball Corp., and IBM. Johnson & Johnson, moreover, entered into a $70 million settlement with the government, while JCG Construction settled for $218.8 million. To give these numbers some perspective, in 2004 the government collected $11 million relating to FCPA violations, and that

which require payment of bounties for tips that lead to recoveries, could have a significant impact on compliance and reporting processes for public *and private* companies.'' (Emphasis added.) Exactly how and why the new rules impact, without stated limitation, private companies was far from clear, however.

Sean McKessy, Chief of the SEC's Whistleblower Office, speaking on a June 15 panel discussing the impact of the rules, commented on this foundational issue. McKessy noted that what we will refer to as ''non-covered companies'' (that is, companies that are not publicly traded and do not otherwise participating in capital markets in a way subjecting them to securities laws) are, indeed, *not* implicated by the new rules. More specifically, McKessy, responding to a question on what impact the new rules have on purely privately held companies, stated, ''the Rules apply to possible violations of federal securities laws . . . there has to be some possible indication that a federal securities law has been violated. A purely private issuer who in no instances is engaged in conduct that could be deemed as a possible violation of federal securities laws would not fit within that definition.'' In response to the question of ''what if you are a private company, but for some reason you have to file something with the SEC because you issue debt—does that bring you under the whistleblower provisions?'' McKessy answered, ''I would say yes.'' That said, most of the observations contained in this article apply to both public and private companies, because, for the reasons discussed below, company internal reporting is generally preferable.

[3] *See* H.R. 5366.

T. Markus Funk is a partner at Perkins Coie LLP and a member of the firm's Investigations & White Collar Defense group. Funk served as an Assistant U.S. Attorney in Chicago for 10 years, is a member of the BNA Criminal Law Reporter advisory board, and serves as the Co-Chair of the ABA's Global Anti-Corruption Task Force. He can be reached at mfunk@perkinscoie.com.

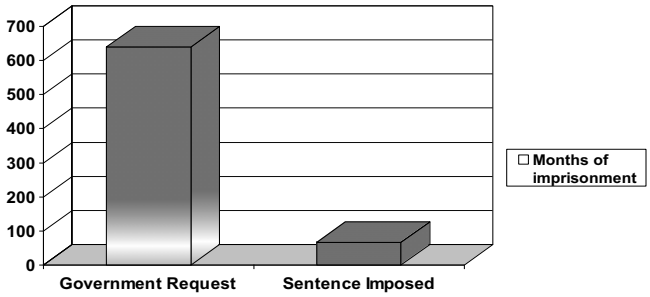
Assad H. Clark, who received his juris doctor degree from Northwestern University School of Law, is an associate at Perkins Coie in the Chicago office. He can be reached at assadclark@perkinscoie.com.

[4] *See generally*, T. Markus Funk, *Don't Pay for the Misdeeds of Others: Intro to Avoiding Foreign Third-Party FCPA Liability*, 6 WCR 33 (Jan. 14, 2011).

  WCR ISSN 1559-3185

amount, at the time, represented an above-average haul.

Although U.S. prosecutors have not always been particularly successful at sentencing (see chart below), if the government continues to use more aggressive investigative approaches and the other strategies described above, and continues its root and branch enforcement reform efforts, it will be perfectly situated to bring more factually and legally compelling cases, which, in turn, will likely result in lengthier sentences.



United States the Clear Leader. A survey of anti-corruption efforts outside U.S. borders shows that, while many countries have finally taken steps to narrow the performance gap, the United States continues to be the world's clear anti-corruption leader. In 2010, for example, the United States again outpaced the rest of the world's collective enforcement efforts by a 3:1 ratio. The United States continues to file more than 70 percent of the world's foreign anti-bribery charges. The latter figure appears even larger when we look at the United Kingdom, in second place, with 4.3 percent of world-wide foreign anti-bribery prosecutions.

The SEC's New Rules Stoke The Flames of Compliance

This past May, following a 3-2 vote, the SEC adopted its rules concerning, among other things, individuals who provide tips to the SEC (''whistleblowers''), per Section 922 of the Dodd-Frank Wall Street Reform and Consumer Protection Act. [5] Of particular note, the SEC has now implemented its hotly anticipated whistleblower bounty program, which rewards individuals who provide the SEC with ''original'' information leading to successful enforcement actions netting more than $1 million in civil *or* criminal monetary sanctions. Eligible whistleblowers can, in fact, earn handsome payouts of 10 to 30 percent of any monies collected because of the tipster's information.

The rules are also notable because of their rejection of the internal reporting mandates for which corporations had so forcefully advocated. As a substitute, the rules:

- include in the awards calculation other misconduct unearthed as a result of the whistleblower's tip;
- create a ''look back'' period to allow whistleblowers to hold their ''place in line'' if they first report their concerns internally to the company—provided the whistleblower subsequently reports that same tip to the SEC within 120 days; and
- announce that the SEC will consider higher percentage bounty awards for tipsters who report potential violations internally before turning to the SEC.

These ''compromises'' are meant (1) to offer meaningful consideration to companies with robust, effective compliance and ethics programs, while (2) concurrently tweaking its whistleblower bounty provisions to lure in additional tipsters. In practice, however, these two objectives can operate to undercut each other, since in their effort to encourage direct reporting to the government, the rules threaten to undermine carefully constructed internal compliance infrastructures.

Who Is Included . . . And Who Is Not

Those potential whistleblowers excluded by the rules include:

- individuals with a pre-existing legal or contractual duty to report their information to the SEC;
- directors, officers, trustees, or partners of an entity who are informed by another person of allegations of misconduct, or who learn the information in connection with the entity's internal reporting mechanisms;
- counsel who obtain the information through a communication subject to the attorney-client privilege;
- compliance and audit personnel;
- individuals who obtain the information through a violation of federal or state criminal law; and
- public accountants who obtain the information through performance of an engagement required of an independent public accountant under federal securities laws.

That said, certain broad *exceptions* to the above-mentioned exclusions significantly narrow the exclusion's otherwise broad scope. These include:

- individuals with a reasonable basis for believing the company is engaging in conduct that will impede an investigation of the potential violation;
- individuals with a reasonable basis for believing that disclosure is necessary to prevent the company from engaging in conduct likely to cause substantial injury to the company's or investors' financial interests, or property; and
- individuals who waited 120 days after internally reporting the misconduct.

The last exception—the ''120-day exception''—is particularly critical in that it forces relatively quick action on the part of companies. This can be especially problematic with allegations involving more widespread misconduct that require broad fact-gathering operations across business units or locations.

The recent establishment of websites such as India's innovative ipaidabribe.com (which, according to reports,[6] has already logged in more than 10,000 incidents of bribery relating to U.S. and other companies since its creation in August 2010) and the U.S.-based http://secwhistleblowerclaimscenter.com, as well as government hotlines such as the SEC's Complaint Center (http:///complaint.shtml), provide ready evidence that attorneys throughout the world see the substantial financial promise in bounty provisions such as those developed by the SEC.

[5] Full text of the rules *available at* http://www.sec.gov/rules/final/2011/34-64545.pdf.

[6] *See* http://www.csmonitor.com/World/Making-a-difference/Change-Agent/2011/0623/I-Paid-a-Bribe-may-be-a-model-for-anti-corruption.

Fuel to the Fire. The SEC's extensive new rules have, in short, added fuel to the already radiating compliance wildfire, promising to motivate even the most lackadaisical compliance officer to review, revise, and rev up his or her anti-compliance framework and training regimen. After all, a compliance program that fails to persuade tipsters to first raise their concerns internally is of little use. Although having a robust, well-thought-out anti-corruption policy in place continues to be a good start, by itself, such a ''paper only'' policy becomes increasingly risky each year. Under the new reporting landscape, companies are, therefore, well advised to take proactive measures not only to ensure the effectiveness of internal compliance programs, but to make internal reporting the most attractive first step for would-be tipsters.

The potential responses sketched out below fall into three broad categories: (1) actions to enhance a company's already existing compliance department, (2) steps to identify any potential violations and to incentivize employees to report those violations to the internal compliance department, and (3) strategies to prevent employees who report violations to the SEC from feeling that the company is not sensitive to the employees' concerns or, worse, is acting in a retaliatory manner. Below are some measures companies can follow to help promote these objectives.

How to Incentivize First-Step Internal Reporting

Tipsters who bypass internal reporting mechanisms and head straight to the SEC, or—as is more likely the case—to the burgeoning group of U.S. and foreign lawyers who see the whistleblower bounty incentives as a ready source of business, prevent companies from (1) immediately investigating the alleged misconduct, (2) evaluating the merit and seriousness of the allegations, and (3) taking appropriate corrective action before the problem can expand even further and cause additional, and potentially irreparable, damage to the company and to others.

Although these and other points were brought to the attention of the SEC prior to the rules' issuance, the SEC in its final analysis did not agree. According to the Commission, ''whistleblowers are in the best position to assess whether reporting potential securities violations through their companies' internal compliance and reporting systems would be effective.''[7]

This official position gives surprisingly short shrift to the policy advantages of permitting companies to promptly address potentially devastating (and often ongoing) internal problems—something the government, given its limited resources and an ever-growing pool of tipsters, may not be in the best position to do. Nevertheless, the rules are the rules, and companies should, therefore, consider taking the following steps to motivate/incentivize their employees to turn *first* to the internal compliance mechanisms.

■ **Review all policies to ensure that (1) reporting obligations and (2) means of reporting violations are as clear and straightforward as possible.** All anti-corruption trainings, codes of ethics, anti-corruption policies, and transaction partner agreements should be written in plain language (and be made available in the language of every country in which the company does business) so all employees can understand what is being said and what responsibilities they have in situations that might result in violations.

The modest cost of such a holistic review is money well spent. This conclusion is, in fact, backed up by Breuer, who remarked, ''We know when we see good compliance. We have a good sense of whether it's robust and real or created on the cheap. . . . [I]t's stunningly bad business not to have a state-of-the-art compliance program. You'll get a better deal.''[8]

Lengthy ''all-things-considered'' paper policies written in legalese simply fall short of the mark. Most anti-corruption violations, after all, are not committed by lawyers, so it is important that managers and employees within all segments of a company know what behavior is forbidden.

■ **Ensure that 800 numbers and compliance officer contact information is readily accessible and provides for anonymous reporting.** Companies should consider substituting anonymous 800 numbers and e-mail reporting addresses such as ''compliance@XYZCorp.com'' for numbers and addresses of named compliance officers. These steps further the impression that the reporting process is handled anonymously. Moreover, companies should explicitly, and prominently, note that (1) anonymous reporting is perfectly acceptable, and (2) the company will not tolerate any adverse employment action against genuine tips by bona fide whistleblowers (more on this below).

■ **Promote a company's compliance programs through compliance workshops and videos**. Companies should ensure that employees and third-party agents are informed about the company's *genuine* ''from the top down'' commitment to maintaining meaningful compliance programs, and to proactively investigating reports. Any annual compliance videos or presentations should be ''decoded'' for the layperson, and should consider real-world ''Frequently Asked Questions,'' along with a short quiz, to ensure that the disseminated information is actually being absorbed.

■ **Instill the proper corporate culture at all levels.** It is important that officers and supervisors are appropriately trained about compliance issues from a managerial perspective. In most cases, supervisors are the ''first responders.'' What may start out as a relatively minor work-related dispute can, if not addressed properly, mushroom into a disgruntled whistleblower action. It is, therefore, critical to make the employee feel that his or her grievances are taken seriously, and that the company is formulating an appropriate response. Accordingly, supervisors must be trained on how to properly address employee complaints.

■ **Incorporate compliance responsibilities into necessary duties and responsibilities of all employees . . . and appropriately *reward* adherence.** Directors, officers, managers, supervisors, and employees should have explicit reporting obligations and an understanding of the company's commitment to a genuine culture of compliance. More than that, however, the company should make clear that a demonstrated compliance

[7] *See* Peter J. Henning, A Greater Incentive for Whistle-Blowers, *Dealbook* (May 26, 2011).

[8] *See* Breuer's remarks at Practising Law Institute (Nov. 4, 2010), available at http://www.justice.gov/criminal/pr/speeches/2010/crm-speech-101104.html.

  WCR ISSN 1559-3185

commitment is part of the performance criteria used in their periodic assessments (while carefully warding off potential retaliation claims by not *punishing* those who fail to first report internally, and, conversely, not exposing itself to allegations that it *de facto* is bribing potential whistleblowers to keep them quite). Providing incentives for reporting through performance-based bonuses can be one way to motivate a company culture of internal reporting.

■ **Avoid the appearance of retaliation.** Companies must always remain mindful that the Dodd-Frank Act also provides strict anti-retaliation provisions and should, therefore, explicitly advise employees that good faith reports will not result in adverse employment action. Although rewarding employees for first internally reporting potential violations should be encouraged, conversely, companies must be mindful that any punishment meted out against employees, regardless of culpability, who bypass the company internal reporting mechanisms could well be interpreted as retaliatory.[9] This is even more critical when the tipster—possibly to preempt appropriate corporate disciplinary action—reports potentially criminal conduct in which the tipster was him or herself involved.[10] In certain situations, disciplinary actions against a tipster may be warranted, but it is paramount that the company ensure that all of its reasons are appropriately considered and documented. Properly documenting all evidence of employee misconduct and creating a substantive paper trail will help insulate the company against subsequent bad-faith retaliation claims the offending employee may assert after he or she has been disciplined or terminated.

■ **Promote the neutrality and fairness of the compliance department.** Consider creating an ombudsperson-type position in connection with the compliance department so that employees are provided with enough assurance that compliance staff will fairly deal with any tips, and are not simply on the ''side of the corporation.''

■ **Review compliance issues without delay and properly document all compliance actions**. Under the SEC's new whistleblower rules, individuals are eligible for a reward only if they give the Commission ''original'' information. It is, therefore, important for a company to be able to demonstrate to the SEC (or DOJ) that it opened a genuine investigation into a compliance matter before the tipster brought his or her complaint to the government. By taking these steps, the company puts itself in the best position to receive appropriate credit for its disclosure. Remember that, as discussed above, companies have only 120 days from the time they receive a tip to report it to the SEC. The company must, therefore, carefully balance the need to act prudently and investigate claims thoroughly against the need to meet this ''first-in-line'' deadline.

Companies should consult with their compliance team and outside counsel to develop a tailored plan of action enabling the company to respond quickly and appropriately to all substantive tips, and to put out compliance fires as quickly as possible (or, if appropriate, to report the problem to the government before anyone else does).

■ **Consider the uncertain benefits of educating employees on the SEC's cash incentives**. Although some have suggested that employees should be fully apprised of the enhanced financial bounty awaiting those who first report internally, most companies, for good reason, will be reluctant to vigorously advertise the potentially vast cash rewards awaiting employees who blow the whistle on their employer. In short, while compliance certainly is a good thing, going out of one's way to affirmatively *generate* tipsters through the lure of potential riches, courtesy of the government, may not be the best business decision. Instead, companies should neutrally advise employees that the government ''encourages tipsters to use the company's internal compliance mechanisms to report suspected misconduct.'' This factually accurate statement advises employees that they should first report internally, while not (1) threatening those who do not or (2) putting excessive emphasis on the cash awards offered by the government.

■ **Be responsive to whistleblower concerns**. Though the financial bounties potentially awaiting successful whistleblowers may fuel the cynic's belief that all tipsters are acting simply out of greed, many tipsters make good-faith reports and are genuinely troubled by what they believe they have discovered. By maintaining open lines of communication between the tipster and the company, compliance personnel help reduce the chances the tipster will get the impression that the matter is being ''whitewashed,'' or that his or her concerns are being ignored or minimized.

In this context, only those supervisors with a ''need to know'' should be told about the whistleblower's identity; this not only honors the sensitive nature of the tip, but also reduces the danger that the tipster will be exposed to retaliatory conduct or will otherwise be isolated.

Conclusion

The SEC's rules, as well as the active government's enforcement initiatives, significantly up the ante for compliance officers. Companies that do little more than draft anti-corruption policies and set up paper-only reporting mechanisms, no matter how well intentioned, may be setting themselves up for problems that a bit of additional front-loaded compliance thinking could have avoided. After all, practical, proactive thinking, and an honest 360-degree look at existing compliance mechanisms, can significantly reduce a company's exposure to risk by increasing the odds that employees will put the company's compliance and reporting mechanisms to their intended use. Employees, after all, are most likely to give their employer the initial opportunity to investigate and correct compliance-related issues if they understand that the company (1) is genuinely concerned about corruption, (2) will take employee con-

[9] Note, however, that while the Dodd-Frank Act prohibits retaliation against an employee for legal actions taken by whistleblowers to provide information to the government, it does not restrict actions taken against an employee for other reasons.

[10] Much to the frustration of the business community, the rules do not, per se, exclude culpable individuals from receiving awards. This apparent setting aside of the ''clean hands doctrine'' can threaten to turn an otherwise straightforward disciplinary action into one with potentially retaliatory elements. An individual claiming retaliation may sue in federal court for reinstatement, double back pay with interest, and attorneys' fees. The statute of limitations can extend as long as 10 years from the date of the retaliation.

cerns seriously, and (3) will treat reports fairly and with the appropriate amount of discretion. As compliance officers can attest, this is vastly preferable to having the employee force the company's hand by making the government his or her first ''tip stop.''

  WCR ISSN 1559-3185