LJN LAW JOURNAL NEWSLETTERS

Business Crimes Bulletin ®

An ALM Publication

Volume 20, Number 7 • March 2013

Key Elements of Effective FCPA Remediation: Earning DOJ and SEC's 'High Premium'

Part One of a Two-Part Article

By Jonny Frank and Rex Homme

The Department of Justice (DOJ) and Securities Exchange Commission's (SEC) Guide to the U.S. Foreign Corruptions Act (FCPA) demonstrates, if there any doubt, the importance of timely and effective FCPA remediation. Calling it a "high premium," the DOJ and SEC explain that FCPA remediation can help an organization avoid criminal prosecution and enforcement proceedings; pay reduced penalties and safeguard brand value; and obviate a government-imposed compliance monitor or independent consultant.

It is not just the organization that is impacted by issues arising from poor internal controls. Board members and senior management face substantial embarrassment and damaged personal reputation. Consider also the career damage to business leaders, ethics and compliance officers and internal auditors.

Effective FCPA remediation adds to the bottom line and should pay for itself many times over. According to a survey conducted by the Economist Intelligence Unit, corporations on average lose 2% of earnings to fraud and corruption, or the equivalent of a full week's work. Roughly 20% of companies lose over 4% of earnings, or the equivalent of two weeks' work, and a quarter of those lose over 10% of earnings. These estimates do not include waste, abuse, fines, investigative and legal fees, or higher insurance premiums. Nor do they capture "soft" costs, *e.g.*, management distraction; lost productivity; talent flight, injured customer and supplier relationships; opportunity loss; and erosion of brand value. The Association of Certified Fraud Examiners Report to the Nations finds that effective antifraud programs cut losses in half, saving most organizations millions of dollars in future losses.

High corruption risk correlates to high fraud risk. Companies doing business in emerging markets face higher than average losses absent effective and proactive antifraud program and controls. A Dow Jones study concluded that nearly 60% of companies delay or avoid global business opportunities due to concern over fraud and corruption.

Government expectations are rigorous and, no surprise, the bar continues to rise. The most detailed guidance appears in the attachments to DOJ corporate deferred and non-prosecution agreements. *See, e.g., U.S. v. Tyco* (D.DC September 2012) (non-prosecution agreement) (*Tyco*); *U.S. v. Pfizer* (D.DC August 2012) (deferred prosecution). Additional guidance appears in the DOJ Principles of Federal Prosecution of Business Organization, SEC Enforcement Manual and Chapter 8 of the U.S. Sentencing Guidelines (USSG) and, most recently, the DOJ and SEC FCPA Resource Guide. This article suggests a practical plan for organizations and counsels to meet these expectations.

USSG: Involve Remediation Advisers

The 2011 amendments to the United States Sentencing Guidelines suggest that organizations include professional advisers in their remediation efforts. Remediation is very different from traditional forensic accounting. Remediation experts work in the absence of a specific allegation or suspicion and apply specialized knowledge, skills and training to promote recovery and prevent recurrence.

Select a remediation adviser experienced in working and coordinating with legal teams — while the remediation team should be benefiting from the findings of the investigation team, thorough and timely remediation processes often require a separate, concurrently retained, focused team. The remediation experts should be knowledgeable on the universe of corruption risks, and be experienced in helping lawyers and organizations to identify root causes of misconduct, conduct anticorruption risk assessments, evaluate entity and transaction levels controls and perform forensic audits.

Consider also whether the remediation adviser should come from a different firm than the forensic accountants that assisted in the investigation. Does counsel represent management or the board? If retained by management's counsel, the remediation expert works alongside and helps the remediation team conduct a root-cause analysis and implement new policies, procedures and controls. When assisting counsel to the board, the remediation adviser assesses the design and operating effectiveness of remedial measures akin to that of an independent monitor.

Jonny Frank, a partner in the New York office of the StoneTurn Group, served for 12 years as a federal prosecutor and 14 years as a partner at PwC, where he founded and led the Investigations and Fraud Risks & Controls. **Rex Homme**, a partner in StoneTurn's Chicago office, has over 20 years' experience helping law firms prevent, detect, and investigate fraud and corruption worldwide.

Independence and Privilege

Independence is another consideration. An independent third party assessment of the organization's remediation carries more weight with prosecutors and regulators. Also, the remediation team cannot audit its own work. The government will not consider a remediation adviser to be independent if it develops or implements the remediation plan or serves as the client's advocate.

Maintaining the attorney/client privilege is essential if the remediation efforts might uncover other corporate misconduct. Consider forming two attorney-led work streams: one for investigation and another for remediation. Separate teams enable counsel to waive privilege to report on remediation while protecting privilege for the investigation. Separate teams also ensure proper allocation of skill sets and avoid the remediation delays that invariably occur when the investigation team is too busy to focus on remediation. Although the teams will be operating separately, coordination is essential and is best achieved if the remediation team communicates processes and results to the lawyer heading the investigation team to ensure that remediation efforts remain in tune with the investigation findings.

Do Not Delay or Wait Until End of Investigation

Government expectations are clear: Commence remediation immediately. Do not wait until the investigation is complete. It is one thing to assert that the organization will take steps to prevent recurrence; it is quite another to prove that those steps have been identified, considered and put into action, albeit preliminarily, as the investigation progresses.

The DOJ and SEC specifically consider whether an organization remediates promptly in determining whether to file charges or impose a monitor. DOJ policy even allows timely remediation to cure compliance program flaws that gave rise to the misconduct. Even if it cannot avoid prosecution, timely remediation substantially reduces the USSG culpability score, potentially saving millions of dollars in fines and penalties.

Some attorneys and organizations delay remediation until the investigation is complete. This is a mistake. Delay allows for the risk of continued violations, thereby exposing the organization to harsher sanctions and likely imposition of a government compliance monitor or independent consultant. Delay also creates a practical challenge apart from legal implications. Internal investigations are physically, emotionally and financially exhausting: sooner or later, management presses for "closure." The appetite for remediation is invariably diminished over time, or even lost.

Root Cause Analysis

The "Cressey Fraud Triangle," named after 1950s criminologist Donald Cressey, provides a useful and simple framework for conducting a root cause analysis in simple matters.

According to Cressey, three conditions exist whenever misconduct occurs: 1) incentive or pressure; 2) opportunity; and 3) rationalization. The analysis thus considers motivation(s) and justification(s) for paying bribes, as well as control gaps that enabled unauthorized use of company assets. The analysis also considers how a "good person" justified the misconduct and whether they feared detection.

Complex or significant misconduct warrants deeper analysis, most frequently, the COSO Internal Controls Framework. (COSO is an acronym for the Committee of Sponsoring Organizations of the Treadway Commission. Information about COSO is available at www.coso.org.) The COSO framework is globally recognized and expressly approved by the SEC as an appropriate framework for identifying and mitigating risks.

The COSO Internal Controls Framework typically depicted as a cube, available on the COSO website. The top of the cube represents organizational objectives. FCPA implicates all three:

Compliance refers to conformity law, which, with respect to corruption, includes violation of the U.S. FCPA as well as foreign and local laws; 2) *Financial Reporting* is almost always an issue since organizational invariably misclassify bribes as legitimate expenses; and 3) *Operation* refers to maximizing earnings through effective and efficient operations. Organizations typically fund bribes by taking advantage of weak operational controls, which, as a practical matter, expose the organization to internal fraud and embezzlement as much, if not more, to FCPA risk.

The side of the COSO cube teaches that the analysis must extend beyond corporate and drive to individual business units and functions. It entails an analysis of the control environment, risk assessment, control activities, information and communication, and monitoring.

Control Environment refers to the corporate culture, including commitment to integrity, "tone at the top," codes of ethics and conduct, mechanisms to report misconduct, training, etc. The root cause analysis should consider how the control environment may have contributed to bribe paying.

Risk Assessment is "fundamental," say the DOJ and SEC in the FCPA Resource Guide, to an effective anticorruption ethics and compliance program. A corruption root cause analysis considers the organization's risk assessment process, whether it anticipated the bribe risk and, if so, linked and evaluated the response. Remediation must correct weaknesses or deficiencies in the risk assessment process to ensure that the organization properly anticipates and addresses future risks.

Control Activities refer to preventive and detective transaction-level controls and "design" and "operating" effectiveness. Most bribery schemes involve flawed internal controls. A proper root cause analysis determines whether the flaw was a matter of design effectiveness, operating effectiveness, or both.

Information and Communication refers to the information systems existing within an organization and how these systems communicate with one another as well as with employees who utilize and interpret the systems. This element also refers to the effectiveness of forensic data analytics to prevent and timely detect corruption. The root cause analysis should assesses the effectiveness of the information systems and communications, including the quality of the organization's antifraud and corruption knowledge management program.

Monitoring and Auditing includes contemporaneous and after-the-fact reviews to detect misconduct "risk factors" and "risk indicators" and to identify whether the controls are effective in addressing them. Risk factors are circumstances that impact likelihood of misconduct occurring — *i.e.*, a high score from Transparency International heightens risk of corruption. Risk indicators are "red flags" that the bribery has or is occurring — *i.e.*, offshore payments to a third party. The root cause analysis should consider the quality of the company's monitoring and auditing systems and whether the misconduct was timely detected.