DODD-FRANK WHISTLEBLOWER PROVISIONS

A CRITICAL LOOK AT MINIMIZING YOUR COMPLIANCE RISK

MIKE ROST
VICE PRESIDENT, MARKETING
THOMSON REUTERS GRC
INTRODUCTION

The passage of Dodd-Frank and the subsequent proposed rules outlined by the SEC created an interesting set of challenges and concerns for internal audit, compliance and legal professionals. Section 922 of Dodd-Frank, which added Section 21F to the Securities and Exchange Act of 1934, specifies that a person who provides the SEC “original information” regarding fraud or securities violations within a company that leads to an enforcement penalty of $1 million or more may be entitled to collect between 10 and 30 percent of the penalties. The provision also provides substantial retaliation protections for whistleblowers.

This raises the concern that incentives could potentially undermine internal audit and corporate compliance systems by encouraging employees to bypass their existing compliance and audit programs and go straight to the SEC with issues. Although the proposed guidelines provide a provision for a 90 day grace period for issues to be reported internally, the law leaves the definition of an effective compliance program open for interpretation. Moreover, the proposed rules provide that no person may take any action to impede a whistleblower from communicating directly with SEC staff about a potential securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement.

WHAT IS A WHISTLEBLOWER

The way the law and the proposed rules are written, the definition of an eligible whistleblower is very open. Outside of attorneys and audit and compliance professionals, most employees will qualify as eligible whistleblowers, even if they are personally involved in the wrongdoing. The proposed rules stipulate that:

“... a whistleblower is an individual who, alone or jointly with others, provides information to the Commission relating to a potential violation of the securities laws. A whistleblower must be a natural person; a company or another entity is not eligible to receive a whistleblower award.”

In defining an eligible whistleblower, the law outlines several key criteria related to the whistleblower having original information, independent knowledge, and reporting the information voluntarily. The proposed SEC rules define these key criteria as:

ORIGINAL INFORMATION: Original information means information that is derived from the whistleblower’s independent knowledge or analysis; is not already known to the Commission from any other source, unless the whistleblower is the original source of the information; and is not exclusively derived from an allegation made in a judicial or administrative hearing, in a governmental report, hearing, audit, or investigation, or from the news media, unless the whistleblower is a source of the information.

INDEPENDENT KNOWLEDGE: Independent knowledge is factual information in the whistleblower’s possession that is not obtained from publicly available sources. Publicly available sources may include both sources that are widely disseminated (such as corporate press releases and filings, media reports, and information on the internet), and sources that, though not widely disseminated, are generally available to the public (such as court filings and documents obtained through Freedom of Information Act requests). Importantly, the proposed definition of “independent knowledge” does not require that a whistleblower have direct, first-hand knowledge of potential violations. Instead, knowledge may be obtained from any of the whistleblower’s experiences, observations, or communications (subject to the exclusion for knowledge obtained from public sources).

VOLUNTARY SUBMISSION: The whistleblower or his representative (such as an attorney) must come forward with the information before receiving any formal or informal request, inquiry, or demand from the Commission staff or from any other authority described in the proposed rule about a matter to which the whistleblower’s information is relevant.
WHO IS EXCLUDED

Those who do not qualify as eligible whistleblowers are typically excluded due to not having independent knowledge or original information, or by the nature of the position that they hold in the organization. Examples of exclusions include:

- Attorneys who have received information through a communication that is subject to the attorney-client privilege.
- Attorneys who obtain information as a result of the legal representation of a client on whose behalf the whistleblower’s services, or the services of the whistleblower’s employer or firm, have been retained, and the person seeks to make a whistleblower submission for his or her own benefit.
- Public accountants are excluded for information obtained through the performance of an engagement required under the securities laws by an independent public accountant, if that information relates to a violation by the engagement client or the client’s directors, officers or other employers.
- Persons with legal, compliance, audit, supervisory or governance responsibilities for an entity who receive information about potential violations, and the information was communicated to the person with the reasonable expectation that the person would take appropriate steps to cause the entity to respond to the violation.

Although the proposed rules declare exclusions for internal compliance staff, there are exceptions. For example:

- An internal auditor who discovers possible securities wrongdoing while performing an internal audit may proactively report it to the SEC in case the company is slower than is deemed reasonable in reporting it to the SEC (if indeed such reporting is warranted).
- If an individual believes that his or her report to the company’s compliance department may enable a member of that department to obtain the bounty as a whistleblower, the individual may avoid submitting the report internally rather than take the risk of someone else receiving the award.

Given the potential size of the bounty, some whistleblowers may decide to take no chances and avoid the internal program altogether.

THE PRECEDENT FOR WHISTLEBLOWER PAYOUTS AND PROTECTION

The concept of whistleblower protection and the compensation for information is not new. Prior to Dodd-Frank, the most visible corporate whistleblower protection laws were initiated under the 1986 amendments to the Federal False Claims act and Section 806 of the Sarbanes Oxley act of 2002.

Under the False Claims Act, 31 U.S.C. §§ 3729-3733, “... those who knowingly submit, or cause another person or entity to submit, false claims for payment of government funds are liable for three times the government’s damages plus civil penalties ...” The False Claims Act contains qui tam, or whistleblower, provisions. Qui tam is a unique mechanism in the law that allows citizens with evidence of fraud against government contracts and programs to sue, on behalf of the government, in order to recover the stolen funds. In compensation for the risk and effort of filing a qui tam case, the citizen whistleblower or “relator” may be awarded a portion of the funds recovered, typically between 15 and 25 percent.

SOX section 806 stipulates that “… no company with securities registered with the SEC or any officer, employee, contractor, subcontractor, or agent of such company, may discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment due to providing information related to violations of rules or regulation of the Securities and Exchange Commission, or any provision of federal law relating to fraud against shareholders.”
According to the 2010 Fullbright and Jaworski Litigations Trends Survey, 22 percent of organizations have been subject to an allegation by a whistleblower in the past three years. Of those, 86 percent of claims initiated an internal investigation, 42 percent resulted in regulatory investigations and 46 percent ended up in a third-party proceeding.

Statistics from the DOJ are equally interesting. According to a November 2009 press release, the Justice Department has recovered $2.4 billion in false claims cases in fiscal year 2009 and more than $24 billion since 1986. Furthermore, a majority of these claims were filed under qui tam provisions.

INTERNAL COMPLIANCE PROGRAMS—THE 90-DAY GRACE PERIOD

The SEC was clear to stipulate in the proposed rules that it does not want to undermine current and effective internal programs meant to enforce compliance with SEC rules. According to the SEC, “… compliance with the federal securities laws is promoted when companies implement effective legal, audit, compliance, and similar functions. Internal compliance and similar functions, when effective, can constrain the opportunities for unlawful activity.”

Given the policy interest in fostering robust corporate compliance programs, the SEC has outlined the approach of encouraging potential whistleblowers to utilize in-house complaint and reporting procedures, thereby giving employees an opportunity to report misconduct, before they make a whistleblower submission to the SEC.

According to the proposed rules, a whistleblower has a 90-day grace period following a report to their company’s internal compliance program. During this time, the whistleblower can alert the SEC and still be considered to have provided original information as of the date of the report to the internal compliance program.

It is significant to point out that the proposed rules do not require an individual to report a potential violation internally to the company as a prerequisite to being an eligible whistleblower. Rather, the proposed rule attempts to accommodate companies’ interest in effective compliance programs by providing stipulations. When determining the amount of an award, the SEC may consider whether a whistleblower reported the potential violation through effective internal whistleblower, legal, or compliance procedures before reporting the violation to the SEC.

MINIMIZING WHISTLEBLOWER RISK—THE IMPORTANCE OF AN EFFECTIVE COMPLIANCE PROGRAM

The natural conclusion that many organizations will reach is that they need to invest in audit, risk and compliance programs to minimize whistleblower risk. As it relates to the whistleblower provisions, strong and effective audit, risk and compliance programs have the potential to deliver two significant benefits. First, they will function as a set of detective controls to uncover fraud or wrongdoing in early stages. Secondly, they will demonstrate to the SEC that the corporation invested in a proper compliance and control environment which may minimize penalties for any wrongdoing uncovered.

This raises the important question of what defines an effective compliance program. A starting point in answering this question is to simply refer to the U.S. Federal Sentencing Guidelines. The guidelines first defined an “effective” compliance program in 1991. This quickly became a starting point standard within the corporate compliance community.

Recently amended in April 2010, section §8B2.1 of the guidelines outline the attributes of an effective compliance program. A summary of these attributes include:

- Establishing a culture of compliance and tone at the top
- Documented standards and procedures (policies)
- Awareness and understanding of compliance requirements
DODD-FRANK WHISTLEBLOWER PROVISIONS - A CRITICAL LOOK AT MINIMIZING YOUR COMPLIANCE RISK

- Communication and reporting
- Risk assessment
- Control definition and monitoring
- Testing and oversight
- Continuing maturity

The challenge with these guidelines is that their definition of an effective compliance program is broad in scope and definition. To predict how the SEC may evaluate an effective program during an enforcement action, it is important to consider how the SEC has historically communicated on effective compliance programs. The SEC looks at compliance as “… a proactive method to identify and control risks that have the potential to result in violations of the law - violations that would result in investor harm and financial and reputational losses at a firm.” An effective compliance program can prevent the potential risks from materializing into violations.

When conducting an evaluation of a compliance program, the SEC will most likely review the following:

- What are the compliance functions at the firm? Do they cover all businesses?
- Does the firm have effective compliance policies and procedures?
- Is compliance independent from business, both in reporting and compensation?
- Do they have access to top management and the board?
- Does compliance have adequate resources, systems and reports?
- Do compliance personnel have appropriate expertise and experience? How are they trained? Are they adequately compensated?
- Does compliance have the ability to respond to and coordinate with all relevant regulators?
- How are new compliance issues and requirements communicated to all personnel?
- How are the concerns of compliance and breaches addressed?

PRACTICAL GUIDANCE—FOUR STEPS TO A MORE EFFECTIVE COMPLIANCE PROGRAM

Considering the whistleblower incentives and the probability of increased enforcement actions by the SEC, it has never been more important to invest in and maintain an effective compliance program. The remainder of this whitepaper discusses four primary areas to address to improve the effectiveness of your internal compliance program. These areas include:

- Managing compliance risks
- Policies and procedures
- Collaboration across assurance groups
- Investing in technology

MANAGING COMPLIANCE RISKS

Assessing and managing risk is a common denominator across all business functions. An important part of any effective compliance program is investing in the discipline of identifying and mitigating compliance risks. To effectively manage compliance risks, it is essential for compliance personnel to stay informed of the latest changes in regulations and enforcements around the globe that may have an impact on them, their senior management and their firm. Keeping track of regulatory themes and trends in enforcement allows compliance departments to proactively manage risk and steer clear of potential enforcement activity.

Effective management of compliance risks may be done through a general risk analysis, self-assessments, branch exams, audits of compliance functions, new product reviews, and surveillance. For all of these activities, it is important to leverage a standard methodology and to have systems in place to document these risks, the relative assertions and assessments, mitigating controls, and any issues and action plans related to surveillance, assessments, and audits. Leveraging a purpose-built technology solution can provide a single repository for all risk
information providing all assurance groups the opportunity to leverage one risk assessment. By standardizing on a single technology solution, business process owners have a complete view of all risk data and executives have visibility into the business risks and opportunities both of which lead to enhanced strategic decision making.

POLICIES AND PROCEDURES
When assessing the effectivity of a compliance program, SEC compliance audits may seek out a review of written supervisory procedures. To effectively address this requirement, the company should have a system to identify all relevant laws and rules and to continually update the related policies and procedures. Compliance may work with the company’s supervisors - those with day-to-day business line responsibility for compliance with the law - to ensure that written supervisory procedures are reasonably designed to achieve compliance with all applicable laws.

Three elements are necessary to optimize your compliance program: access to the most up-to-date changes in laws and regulations; a mechanism to make changes to policies and procedures; and a process to communicate those changes to employees. This includes the requirement to manage the creation, management, and enforcement of your compliance policies and procedures at every lifecycle phase: create, edit, review, approve.

An archive of past and current policies provides for successful recordkeeping and the ability to quickly reference policies during an episode of enforcement. If confronted with an enforcement action, having an instant snapshot and record of the policies in force at any previous date and an audit trail of which personnel have read and accepted said policies will be extremely valuable.

Finally, an effective compliance program provides a mechanism for all staff to be informed and trained on relevant policies and procedures. Training strengthens an organization’s compliance culture and educates the business lines and senior management on regulator expectations. Training also helps to significantly mitigate the risk and expense of regulatory failure. Effective compliance programs typically have some form of classroom or e-learning courses that cover the spectrum of topics that have been highlighted for enforcement.

COLLABORATION ACROSS ASSURANCE GROUPS
Driven by internal reporting structures, direction from senior executives, and traditional functional roles; internal audit, risk management, and compliance professionals often work in very rigid silos focused on a tactical set of departmental objectives. Too much white space exists where information is not exchanged and accountability is not established among assurance groups. Based on the provisions of the proposed whistleblower rules, it is critical that all whitespaces and communication gaps are eliminated between audit, risk and compliance groups to improve the effectiveness of the detective controls of the organization.

Coordination between assurance groups is best achieved by leveraging a common language of risk and control and a common methodology between groups. A comprehensive assessment of risks and controls requires the use of standard risk and control taxonomy. Effective GRC collaboration requires that risks and controls be classified and reported against standard models on which GRC groups agree. The benefits of utilizing a common language for risks and controls are far reaching and include:

- Improved reporting throughout the organization
- Consistent coverage – all risks are considered
- Improved business performance – risks explain performance gaps
- Better decision making – decisions are risk based
- Less external oversight and audits – controls are standardized

A common methodology for compliance, audit and risk groups leads to agreement about what and how information must be gathered, how to define the risk types to assess and the risk thresholds to drive the depth and quality of the review. Effective compliance programs define the thresholds beyond which risks would require mitigation or additional management, definitions of what controls require testing, and rules governing the creation of issues for reporting and resolution.
LEVERAGING TECHNOLOGY

The pursuit of an effective compliance program is not a technology or IT initiative. However, organizations on the leading edge of managing compliance rely on comprehensive information technology that addresses all of the requirements of an effective compliance program.

A natural outcome and a potential driver of a siloed approach to managing compliance and control processes is using different technology solutions to manage each discrete assurance area. With this approach an organization runs the risk of inconsistencies and inefficiencies that may lead to unnecessary high costs. Multiple systems with multiple deployments cause conflicting versions of the truth. A standardized solution resolves these problems and establishes a single version of the truth for the entire enterprise.

Standardized technology provides greater efficiency, improves collaboration, and reduces the time and resource costs associated with compliance processes. Investment in technology enables organizations to break down the walls between audit, risk and compliance groups and provides expanded value as organizations deploy the software across the enterprise. By unifying the many business process owners, a comprehensive software solution can eliminate information silos, redundant data entry and improve information transparency and communication.

The outcome of technology investment is that compliance, internal audit and risk management teams will leverage information and processes into a unified framework that will result in:

- A shared repository of compliance information used for managing regulations, policies and procedures, and addressing enforcement actions.
- A common calibrated methodology allowing collaboration among compliance, audit and risk professionals and the ability for each group to rely on the work of others.
- Searchable knowledge to enable all compliance information to be analyzed and reported.
- A framework for real time, positive, entity wide reporting of the status and trends of risks and controls across the organization.
ABOUT THOMSON REUTERS GRC SOLUTIONS

Thomson Reuters is the world’s leading source of intelligent information for businesses and professionals. The company combines industry expertise with innovative technology to deliver critical information for leading decision-makers in the financial, legal, tax and accounting, scientific and healthcare markets.

GRC solutions from Thomson Reuters enables decision making across the organization. They combine regulatory intelligence, dynamic market data, risk and control systems, and rich capabilities for anti-money laundering/know your customer insights into a meaningful context. They connect four key areas of business – regulatory risk evaluation; product, transaction, and policy development; compliance processes; and disclosure – with powerful market and regulatory information. Streamed together, they allow an unprecedented level of synergy within the firm. In this new environment, the key activities of the business are dynamically connected with information and operational workflow services from Thomson Reuters.

Learn More
Call: 763.450.4700
Visit: paisley.thomsonreuters.com

ABOUT THE AUTHOR

Mike Rost
Vice President, Marketing – Thomson Reuters GRC Solutions

With more than 20 years experience in assisting organizations in using technology to optimize business processes, Mike Rost is a key contributor to the Thomson Reuters GRC strategy and works with business leaders to promote the adoption of integrated GRC. Mike has over five years experience working with internal audit, risk, and compliance professionals and serves on the Leadership Council and Technology Council of the Open Compliance and Ethics Group. Prior to joining Thomson Reuters, Mike held leadership positions with several technology companies including seven years at Lawson Software in St. Paul, Minnesota. Prior to joining Lawson, Mike spent 8 years in various corporate finance roles working for both Pillsbury and Rollerblade, Inc. Mike is an experienced speaker and presenter participating regularly in international conferences on the subject of audit, risk, and compliance. Mike earned a bachelor’s degree in economics and a MBA in marketing and finance from the University of Minnesota.