Bloomberg BNA

Securities Regulation & Law Report™

Reproduced with permission from Securities Regulation & Law Report, 44 SRLR 922, 05/07/2012. Copyright © 2012 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

WHISTLEBLOWERS

Preparing for the Deluge: How to Respond When Employees Speak Up and Report Possible Compliance Violations

BY WILLIAM MCLUCAS, LAURA WERTHEIMER, AND ARIAN JUNE

In our recent piece, ''Get Ahead of the Bus or Be Hit by the Bus,'' published in March, we discussed the challenges created by the Whistleblower Program for organizations covered by it and offered a number of practical strategies for organizations to consider in meeting those challenges. The Whistleblower Program represents the most recent effort by Congress to incentivize employees and third parties to share information relating to possible misconduct with the government. Those incentives are not surprising in light of studies showing that employees are the most likely group to first detect improper conduct. We recommended that organizations consider a number of complimentary practical strategies to strengthen the internal compliance environment and address employee perceptions regarding the utility and safety of speaking up with compliance-related questions. Those enhancements may reduce the overall risk profile of an organization and should encourage employees to report compliance concerns before any misconduct occurs.

William McLucas is the chair of WilmerHale's Securities Department and a member of the firm's Securities Litigation and Enforcement Practice as well as its Dodd-Frank Whistleblower Working Group.

Laura Wertheimer is a partner in WilmerHale's Securities Department, and also a member of the Securities Litigation and Enforcement Practice.

Arian June is a Senior Associate in WilmerHale's Securities Department, and a member of the Securities Litigation and Enforcement Practice.

We also recognized the need for organizations to prepare for an anticipated increase in internal reports of possible securities violations. How should an organization respond when such a report is received? We previously proposed that organizations consider investing the time and resources to develop a written response plan and identified a number of issues that could be addressed in such a plan. We now turn to discuss each of these issues.

Should all internal reports of compliance concerns and/or possible compliance violations be escalated to one central function?

Many organizations have established processes to track and respond to reports received through anonymous hotlines, suggestion drop boxes, and anonymous e-mail or web-based reporting vehicles. These processes typically tasked internal audit or compliance with responsibility for reviewing and resolving all such reports, regardless of the nature of the complaint. Most organizations, however, have not adopted formal processes to track and respond to reports of compliance concerns or potential compliance violations made to supervisors or managers.

As we discussed in our prior article, survey data consistently shows that an overwhelming number of employees who speak up to report compliance concerns within the organization speak to an immediate supervi-

COPYRIGHT © 2012 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 0037-0665

sor or to more senior managers with perceived authority to remedy the concern.[1] Workplace surveys over the last five years show that employees rarely use anonymous hotlines to report misconduct.[2] But even in those organizations where the senior leadership team sets the appropriate tone at the top and encourages employees to voice concerns, employees who speak up to a direct supervisor and/or manager may perceive that the individual was not willing to listen or act on their concerns or that speaking up was not ''safe.''[3] When managers and supervisors are tasked with the review of and response to employee reports, there are heightened risks that such reports will not be consistently, efficiently and effectively reviewed or investigated, that appropriate remediation will not be adopted, that reported concerns will not be tracked (which impairs an organization's ability to address systemic issues) and that the reporting employees will be intimidated from raising uncomfortable concerns in the future. As a recent study of qui tam relators in the pharmaceutical industry has shown, many employee relators who first self-reported potential compliance violations to managers or supervisors sought redress outside their organizations as a ''last resort'' only after they perceived that little or no action would be taken to investigate their reported concerns and/or that their positions would be in jeopardy.[4] Lack of a formalized process that requires escalation of every internal report of possible compliance violations to one centralized function for review and response increases the likelihood that reporting employees will become SEC whistleblowers (and also increases the potential to expand the pool of SEC whistleblowers if the reporting employee shares his displeasure with the apparent futility of internal reporting mechanisms with other employees).

Over the last decade, many of the well-known corporate scandals were not the result of bad behavior by one or two senior managers but were caused by longstanding inappropriate behavior, either encouraged or accepted by the senior leadership team, and judgments were rationalized on the ground that ''everyone does it.''

An established escalation mechanism for internal reports of compliance concerns and possible compliance violations is a strong control: it should encourage employees to surface potential compliance problems because such problems will be reviewed and addressed by qualified individuals with no involvement in the potential issue; it should permit management to more accurately track and log the progress and resolution of such internal reports; and it should enable management to flag potential organization-wide issues that can then be addressed through improved processes and controls. As such, the escalation mechanism is another tangible demonstration that the organization has ''internalized'' its commitment to compliance.[5]

Once escalated, what function within the organization should make an initial assessment of the internal report?

An initial assessment should be made of each internal report of a possible compliance violation to determine whether it has enough substance to be considered credible and warrant investigation.

- Who are the individuals allegedly involved?
- Are there specific allegations with sufficient information to be believable?
- Do the concerns make sense in light of what is known about the organization and its operations and the employees supposedly involved?
- Do the compliance concerns relate to potential violations of the securities laws, such as accounting and financial reporting matters, bribery and corruption, financial fraud, or insider trading, or do they relate to other compliance issues, such as improper recruitment and hiring practices, conflicts of interest, sexual harassment, or the improper acceptance of gifts?

Assignment of the responsibility to make an initial assessment ought to begin with the end of the process in mind. For the reasons discussed previously, it is reasonable to assume that many employees who report possible compliance violations will become SEC whistleblowers.[6] When the SEC calls, an organization should be prepared to defend what it did. Accordingly, the function assigned responsibility for the initial assessment should be expected to document the scope of its review and conclusions: that it reviewed the internal report and concluded that no further inquiry was warranted, for reasons clearly explained in the supporting documentation; or that it reviewed the report, determined that the concerns were sufficiently credible to warrant investigation, and that an investigation was commenced.

Lawyers in the General Counsel's office may be in the best position in many organizations to conduct the initial assessment because of their substantive knowledge of the securities laws, experience in reviewing allega-

[1] William McLucas, Laura Wertheimer & Arian June, *Get Ahead of the Bus or Be Hit by the Bus: Practical Strategies forMeeting the Challenges and Mitigating the Risks of the Dodd-Frank Whistleblower Program*, 44 SEC. REG. & L. REPORT (Bloomberg BNA) No. 11, 526, at 530 n.21 (March 12, 2012) (44 SRLR 526, 3/12/12).

[2] *Id*. The 2010 Ethics Resource Survey found that anonymous hotlines were used 3% of the time. Ethics Resource Center, *Blowing the Whistle on Workplace Misconduct*, 5 (December 2010). We do not intend to suggest that anonymous hotlines do not provide a valuable resource. For example, a large U.S. public company reported to the Ethics Resource Center that it received ''an average of 431 hotline tips every month and that, on investigation, almost 20 percent of these lead to findings of misconduct.'' *Id.* at 6.

[3] James R. Detert & Linda K. Treviño, *Speaking Up to Higher-Ups: How Supervisors and Skip-Level Leaders Influence Employee Voice*, 21 ORGANIZATION SCIENCE, No. 1, 249-70 (January–February 2010).

[4] Aaron S. Kesselheim et al., *Special Report, Whistle-Blowers' Experiences in Fraud Litigation against Pharmaceutical Companies*, 362 NEW ENG. J. OF MED. 1832 (May 13, 2010).

[5] The United States Attorney for the Southern District of New York, Preet Bharara, keynote speaker at Compliance Week 2011, stressed that ''the best-conceived compliance programs, and practices and policies in the world will be too weak to stave off scandal if the core principles are not internalized, if there is not from the top a daily drumbeat for integrity.'' Jaclyn Jaeger, *Compliance Week 2011: Enforcers Talk Ethics, and Talk Details, Compliance Week* (June 1, 2011).

[6] William McLucas & Laura Wertheimer, *Responding to a Corporate Crisis—A Framework for Dealing with Bad News*, 3 J. OF SEC. L., REG. & COMPLIANCE, No. 1, 24, 24-25 (2010).

 COPYRIGHT © 2012 BY THE BUREAU OF NATIONAL AFFAIRS, INC. SRLR ISSN 0037-0665

tions and objectivity. When in-house lawyers make the initial assessment, that assessment should preserve applicable privileges. Other organizations may prefer to have the initial assessment performed by internal audit, compliance, or corporate security because these functions may be more experienced in handling employee complaints and may be more knowledgeable about the organization's operations. When initial assessments are performed by non-legal personnel, they are likely to be discoverable in a future litigation dispute, which may create difficulties down the road.

Which types of internal reports of compliance concerns or potential compliance violations should be escalated promptly to the Board of Directors?

Boards of directors are charged with responsibility to oversee an organization's risk management. Where an internal report of serious misconduct is received, such as those involving a material amount of money and/or senior managers, such a report should be escalated promptly to the board of directors. In these circumstances, management should not wait until the conclusion of an initial assessment of the credibility of the internal report before alerting the board of directors.

That recommendation is not meant to suggest that an organization's board of directors, or a committee of its independent directors should initiate and oversee every investigation of such reports. Instead, an organization's written action plan should identify the types of internal reports that would warrant investigation by independent directors and those that would warrant investigation by senior management. For example, an organization could determine that internal reports alleging possible compliance violations that, if proven, could threaten its franchise or involve members of senior management should be investigated under the direction of the independent directors. Reports alleging possible compliance violations where the credibility of senior management is not called into question and senior management is not allegedly involved or otherwise conflicted could be investigated under the direction of senior management or the board of directors, depending on the alleged facts and seriousness of the possible violations.[7]

Which individuals in the organization should be informed about an internal report of possible compliance violations and what information should be shared with them?

In most organizations, there is continual chatter and many employees trade in the currency of information. A written plan for internal investigations should make clear that the identity of the reporting employee (if known), information regarding the initial assessment of the internal report, the need for an investigation, the progress of an investigation and its conclusions will not be shared outside the group of designated individuals to whom the investigators report. Severely restricting the availability of information to this limited group serves numerous purposes. Among other things, it permits the investigators to obtain witness recollections that are not tainted by information gleaned from others. Indeed, investigators should direct every interviewee not to disclose the existence of the investigation or substance of the interview to anyone. It also reduces the risk that ''inadvertent'' whistleblowers will be created—e.g., individuals who lack firsthand knowledge of the facts giving rise to the internal report of possible compliance violations and learn about the issue through internal conversations.

Perhaps most importantly, it reduces the potential for retaliation claims. Whistleblower anti-retaliation provisions apply broadly and retaliatory actions are not limited to discharge, demotion, transfer, suspension, or reassignment of duties. Because retaliation depends on cause and effect, the identity of reporting employees (if known) should be very closely held and managers and supervisors who escalate internal reports of possible violations should not be advised of the initial assessment of that report or of any ensuing investigation.

Should lawyers (whether in the Office of the General Counsel or outside counsel) conduct all investigations of possible compliance violations to best protect the organization's privileges?

Once an initial assessment identifies an internal report containing specific and credible information of possible compliance violations, a competent, thorough investigation of that report is warranted. As long as there have been whistleblowers with facially credible claims, organizations have sought to conduct unbiased, thorough and prompt investigations. Because most organizations will act based on facts found through the internal investigation process, the experience and skill of the investigators is critical. Non-legal employees in internal audit, compliance and human resources departments regularly investigate internal reports of theft, misuse of resources, workplace complaints, and other issues and have a direct understanding of the organization's climate. However, such employees may not have the training and experience to investigate possible violations of the securities laws and/or the tools to review voluminous electronic and hard copy documents. Even where they may be appropriately qualified, investigations conducted by non-lawyers may not be entitled to privilege protections.

When internal investigations into possible compliance violations are conducted by counsel, information gained through interviews of current and former employees (after these individuals are provided with appropriate *Upjohn* warnings) should be protected by the attorney-client privilege. Because this setting poses a heightened potential for regulatory interactions and possible shareholder derivative litigation, protection of an organization's privileges will almost always be of critical importance. Lawyers (whether in-house or out-

[7] Most organizations have established processes to investigate serious issues, such as theft, that do not constitute violations of the securities laws. Those investigations are often assigned to trained investigators in the internal audit or compliance functions. In our view, the Dodd-Frank Whistleblower Program, which is limited in scope to securities law violations, does not warrant review of such processes.

side counsel), in turn, can assemble a team of legal and non-legal investigators (including outside forensic experts) to work at the lawyers' direction, which better ensures that applicable privileges are protected. In addition, use of a lawyer to conduct the internal investigation lessens the risk of expanding the pool of potential whistleblowers because the SEC's rules make clear that lawyers who submit information protected by the attorney-client privilege generally will not be eligible for a whistleblower award unless such disclosure would otherwise be permitted under SEC or state ethics rules.[8]

What types of allegations warrant retention of outside counsel to conduct the investigation?

Internal reports of possible compliance violations can generally be grouped into three categories. The first category includes allegations of misconduct by senior management and/or issues that could threaten the organization's franchise. In these circumstances, the independent directors (or a committee of independent directors) should undertake responsibility for the investigation and should retain outside, independent counsel to assist in that investigation.

The second category—credible allegations of serious wrongdoing which do not involve senior management but could be significant and material to the organization—could be assigned either to senior management or a committee of independent directors to investigate. For this category of allegations, there is no ''one size fits all'' answer to whether in-house counsel or outside corporate counsel should lead the investigation or whether new outside counsel should be retained. In making that determination, an organization should not lose sight of the real possibility that a reporting employee will become an SEC whistleblower and the SEC will likely call upon the organization to explain its investigative efforts and defend its conclusions. Organizations should recognize that even the most well-designed and executed investigation may receive little credit from the whistleblower, other employees, or the SEC when the investigator is seen as too close to management and lacking necessary objectivity and independence to ask hard questions and raise critical issues.[9]

The third category—credible allegations about possible compliance violations involving a few individuals who are not part of senior management—are typically assigned to senior management to investigate. Allegations in this category generally have a narrow focus—for example, employee X traded during a period when the trading window was closed—and involve a limited number of participants. In-house counsel (or outside corporate counsel) are appropriate candidates to conduct such investigations, provided that they had no role in advising the employee being investigated and recognize their obligation to conduct an unbiased and thorough investigation.

Does the internal IT function have the experience and capability to preserve and collect electronically stored information?

Once a determination is made to conduct an internal investigation into a possible compliance violation, an organization must preserve the universe of potentially relevant documents and electronically stored information and promptly develop and implement a plan to collect the materials. The backbone of any effective internal investigation is to preserve, identify and collect the data set from relevant custodians and places, and cull from that mass of material the potentially relevant information. The quality of the fact finding of an internal investigation almost always stands or falls on the thoroughness of document preservation, collection and review. Should regulators become involved, an organization will need to demonstrate its efforts to properly preserve and collect electronically stored information. An inability to make that showing can significantly damage the organization's credibility and ability to defend itself.

In a perfect world, an organization's internal IT function would be completely fluent with the organization's IT architecture—past and present—and be equipped with the necessary tools to facilitate preservation and collection of electronic stored information from numerous sources. But the world is far from perfect. Over the last 10 years, the volume of business documentation has increased exponentially and electronically stored information now includes instant messages, text messages, tweets and other social media, and cloud-stored information such as SharePoint. In most cases, internal IT staffers are fully engaged by the demands of maintaining the smooth operation of the organization's current networks, servers, hard drives and electronic information storage systems. Preserving and collecting electronically stored information from hard drives of current and former employees, current and legacy systems and servers, backup tapes, and multiple other sources, however, requires skill sets different from managing current IT systems and remediating IT issues. It is often difficult for internal IT staff to identify and collect potentially relevant information from archived servers, legacy systems, backup tapes and hard drives. Even the most sophisticated and experienced IT function may not have the staffing complement necessary to handle existing workload demands and to promptly preserve and collect electronically stored information from all relevant sources or to provide outside counsel or e-discovery vendors with rapid access to requested electronic information.

Because missteps with document preservation and collection at the beginning of a fast-moving internal investigation can haunt the entire investigation and create additional, significant problems, organizations should consider whether retention of an outside e-discovery vendor is warranted. Many vendors also offer technological tools and capabilities that allow investigators to effectively and efficiently review the electronic information that has been collected, which is often massive in volume and is not capable of being manually searched in a reasonable period of time.

---

[8] Implementation of the Whistleblower Provision of Section 21F of the Securities Exchange Act of 1934, Release No. 34-64545, at 71, May 25, 2011, *available at* http://www.sec.gov/rules/final/2011/34-64545.pdf.

[9] For a fulsome discussion of applicable considerations, *see* McLucas & Wertheimer, *supra* note 6, at 27-30.

 COPYRIGHT © 2012 BY THE BUREAU OF NATIONAL AFFAIRS, INC. SRLR ISSN 0037-0665

Which individuals or function should be responsible for regularly communicating with the reporting employee, if known, on the progress of the investigation and who should determine how detailed those reports should be?

We discussed previously the practical strategies that organizations should consider to enhance their existing compliance infrastructure.[10] Even where organizations adopt ''best practices'' for internal reporting mechanisms, a failure to advise reporting employees about the progress of an ongoing investigation into a possible compliance violation is likely to create cynicism about the organization's commitment to investigate reports and could lead the employee to report his or her concerns outside the organization. In contrast, when reporting employees are kept in the loop about the progress of the investigation, that process sends the message that the organization values such internal reports, that the reporting employee is respected by the organization, and that the organization intends to get to the bottom of the concern and to deal with it appropriately.

At the outset, the reporting employee could be advised that status updates will be provided by an individual designated by the organization. Others should resist any efforts by the reporting employee to gain additional insights into or information about the investigation. To avoid confusion and mixed messages, it is important that the organization speak with one voice to the reporting employee and in the voice of the designated reporter. Status reports should provide information sufficient for the employee to understand that the organization has not closed ranks to protect management and the status quo, that the on-going investigation is being conducted by qualified, unbiased investigators, and that his or her concerns are being fully reviewed. Upon the completion of the investigation, the reporting employee could be advised whether the allegations were substantiated, and where appropriate, provided with a summary of any remedial actions that the organization is taking.

Organizations should assume that any information provided in status reports to the reporting employee will be passed on to the SEC and scrutinized by it. Inside or outside counsel with familiarity with the investigation may be the best candidate to provide oral status reports to the employee, provided that the contents of the reports can be scripted to avoid potential privilege waivers.

What is the projected timetable to respond to an internal report of a compliance concern or possible compliance violation?

The SEC's whistleblower rules provide individuals who internally report possible violations of the securities laws with a 120-day ''grace period'' in which to submit the same information to the SEC and be deemed to have their SEC submission dated as of the date of their internal report. More than ever before, this regulatory scheme creates substantial pressure on organizations to establish an abbreviated timetable in their written procedures for the escalation and initial assessment of such internal reports. Since whistleblowers (with limited exceptions) do not need to wait until the 120-day ''grace'' period expires to submit their information to the SEC, an organization should prepare for the possibility that it will be contacted by the SEC within 120 days and will be asked to explain what it did in response to the internal report and why that response was adequate.

Organizations, however, should resist the urge to conclude that every internal investigation must be completed within the 120-day grace period. Because the scope of any investigation turns on the nature of the alleged reported violations, it would not be reasonable to set a fixed timetable for completion of every internal investigation. Alleged violations involving complicated accounting for numerous transactions, or for transactions that took place over a period of years, for example, will likely require longer to investigate than an allegation involving discrete misconduct by one employee.

The goal of almost every internal investigation should be to figure out the facts relevant to the alleged violation or misconduct, as quickly as possible. Because few, if any, individuals have a complete grasp of the facts when they internally report a possible compliance violation or misconduct, investigators need to dig sufficiently deep to ensure that they have a full grasp of the relevant facts and the issues. The ''art'' of any internal investigation is to dig deeply enough to make sure that significant issues have not been missed and that facts relevant to the issues have been found but to avoid irrelevant rabbit holes. There is real peril when an organization insists upon reaching conclusions before it has a firm grasp on the underlying facts, as demonstrated most vividly by the recent episode involving Renault.[11] There, Renault received an anonymous whistleblower report alleging that certain senior members of management were involved in corporate espionage for a competitor. After a hasty internal investigation, Renault dismissed three senior managers based ''less on concrete evidence of what the three managers had allegedly done and more 'because [it] estimate[d] that the risks . . . were too big.''[12] Renault then retracted its conclusions less than 2 months later which plunged it into another crisis, more severe than the first.

Because the individual whistleblower controls whether and when to submit his or her report to the SEC without regard to the status of the organization's internal processes, the organization may need to decide whether to self-report a possible compliance violation to the SEC at an early stage in order to maximize available cooperation credit, even though it has not com-

[10] McLucas et al., *supra* note 1, at 528-35.

[11] Ashby Jones & Joann S. Lublin, *In Wake of Renault, Firms Think Twice About Whistleblowing*, THE WALL ST. J., March 4, 2011, *available at* http://online.wsj.com/article/SB10001424052748703327404576194913231712904.html.

[12] Sebastian Moffet & David Pearson, *Renault's Ghosn: Costs Data Key to Spy Case*, THE WALL ST. J., February 11, 2011, *available at* http://online.wsj.com/article/SB10001424052748703310104576134803371815280.html.

pleted its internal investigation.[13] In this circumstance, the SEC will expect the organization to ''cooperate'' by sharing the factual findings and conclusions at the conclusion of the investigation which can implicate otherwise privileged information. However, should an organization determine to come forward and self-report before the whistleblower and agrees to cooperate, it should recognize that the cooperation credit ultimately awarded by the SEC will not be quantified until the end of the process.

Which individuals or function will be responsible for assembling the findings of the investigation and should the findings be reduced to a written report?

The work plan should charge investigators with presenting their factual findings to the individuals delegated the responsibility to oversee the investigation (such as the senior management team, the board of directors, or a committee of independent directors). Depending on the scope of the investigation, the investigators may also be asked to recommend appropriate remedial actions to address the problems found and improvements to controls and processes to better prevent, detect and respond to similar issues in the future. In some instances, improper ongoing activity may be uncovered during the course of an internal investigation. The written work plan should make clear that investigators are expected to promptly bring that information forward so that the organization can stop it.

[13] Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, Exchange Act Release No. 44969 (Oct. 23, 2001).

The investigative findings can be documented in an oral or written report. The advantages of a written report—a detailed presentation of findings—are also its disadvantages. In the event of litigation, with regulators, private parties, or both, the written report may be discoverable. Because a written report may be construed to be admissions by the organization, it may not only provide a road map for plaintiffs in litigation but it may also increase the cost to the organization of resolving any liabilities arising from misconduct.

Conclusion

Internal reports of possible securities violations are never welcome news. As discussed in our previous article, enhancements to an existing compliance infrastructure, including improvements to risk management and governance processes and internal controls, should reinforce a culture of compliance and reduce the risk of inappropriate activity going forward.

However, the possible financial bounties available to whistleblowers increases the likelihood that individuals will speak up and report concerns about past events and activities and submit the same information to the SEC. Organizations should anticipate that conduct that had not been challenged before may now be under a microscope, pressed by individuals with interests different from that of the organization. While the allegations in the internal reports may differ, organizations should anticipate an increase in these types of internal reports and develop a comprehensive written plan of response. Advance planning, with focus on timetables, assigned responsibilities, procedures and strategies, should enable the organization to respond promptly when a report is received with a credible, diligent process.

 COPYRIGHT © 2012 BY THE BUREAU OF NATIONAL AFFAIRS, INC. SRLR ISSN 0037-0665