Portions of Chapter 6 – Why Should Organizations Adopt a Robust Whistleblower System?

THE FIVE PRIMARY REASONS that organizations should adopt a robust whistleblower system are:

1. To protect the organization from criminal indictment, conviction, and fines and from related civil liability

2. To protect the shareholders or other equity holders of the organization from loss of value of their equity interests

3. To protect the board of directors and officers from civil liability

4. To protect the chief executive officer (CEO) from both criminal and civil liability

5. To protect the business reputation of both the directors and the CEO

The purpose of a robust whistleblower system is to induce employees to use the internal compliance system to report illegal activity rather than report such activity externally to receive statutory rewards. Internal reporting permits the organization to prevent and correct the illegal behavior, thereby helping to safeguard the organization and its directors, officers, and equity holders from the consequences of such illegal behavior.

As discussed in this chapter, if a scandal occurs during the watch of a director or CEO, his or her business reputation will suffer, and it will be difficult to seek other comparable positions. This chapter also discusses the potential civil and criminal liability of both the organization and its directors and the CEO.

Many directors and CEOs believe that they and their organizations are protected by creating and disseminating a "paper" corporate compliance policy and designating a person as chief compliance officer. Nothing could be further from the truth. This chapter discusses the case of Charles Park, the CEO of Acme Markets, who did exactly that and still was found personally criminally liable. Although Park-type cases are rare, prosecutors are becoming very frustrated with their inability to change corporate conduct solely through prosecution of the corporation and may elect to bring criminal prosecutions against CEOs and other responsible members of management. This frustration has also led to attempts to oust longtime CEOs, particularly in the pharmaceutical industry.

Both the board of directors and the CEO have fiduciary responsibilities to the corporation, and investors expect the board to have ultimate responsibility for risk oversight. Any failure of corporate compliance may result in a shareholders' suit against both the CEO and the board of directors for the damage they have caused to the corporation. In addition, regulators, such as the U.S. Department of Justice (DOJ) and other federal and state agencies, also may bring direct actions against the CEO and the board of directors for their participation in unlawful activities.

DIMINISHMENT OF SHAREHOLDER WEALTH

Criminal indictment or conviction of an organization has far-reaching negative consequences for the organization. The indictment or conviction results in adverse publicity for the organization and sullies its reputation. Indictment or conviction also may lead to a loss of important customers or suppliers. Governmental and other customers may suspend or bar the organization from doing business. The organization's ability to attract and retain competent executives may suffer. The organization may incur enormous legal fees and costs in contesting the indictment and any related shareholder lawsuits and suffer huge fines and penalties if convicted.

Melissa Baucus and David Baucus studied 68 Fortune 300 firms that were criminally convicted for five years, beginning with the year following the conviction. The study used three performance measures: shareholder returns, return on assets, and return on sales. The 68 firms were then compared, using the same performance measurements, to unconvicted Fortune 300 firms during the same five-year period, controlling the comparison statistically for variables of size and industry membership. The study concluded:

> Convicted firms generate lower accounting returns (ROA [return on assets] and ROS [return on sales]) in the first year and over the five years after a conviction, possibly reflecting lower revenues or higher costs. These firms experience immediate and prolonged reductions in revenues as stakeholders (e.g., customers) exit the firms, and they may incur increased longer-term costs associated with acquiring capital, alleviating employee concerns, and attempting to stop the exodus of customers.
>
> Convicted firms experience reduced sales growth in the period three through five years after a conviction, indicating that customers may react more slowly to wrongdoing than other stakeholders. Managers employ defensive tactics . . . smoothing the immediate impact of convictions on sales by advertising, reducing prices, or shipping products within the fiscal year to overstate revenues. . . . Firms employing defensive initiatives experience immediate decreases in returns; however, defense initiatives and publicity have a temporary positive impact on sales, and the drop in sales shows up in years three through five.
>
> The seriousness of violations did not relate differentially to longer-term performance, suggesting stakeholders paint all convicted firms with the same brush. A conviction may stain a firm's image, sending a warning signal to stakeholders, or prompt stakeholders to reassess relationships with the firm, regardless of its seriousness.

Other empirical studies have supported the thesis that indictment of a public corporation has at least a short-term negative impact on shareholder wealth. Even Securities and Exchange Commission enforcement actions, to say nothing of criminal indictments, can have major negative impacts on share prices.

BOARDS OF DIRECTORS

We now turn to why the board of directors should establish a robust whistleblower system. We begin with examples in which the boards of companies that had disasters were never given the proper information by senior management. We then discuss the legal standard applicable to directors.

The history of corporate scandals during the last 50 years shows that boards of directors, particularly the independent directors, were completely blindsided by impending scandals; they had no prior knowledge that problems were occurring. The independent directors were clueless because they relied on management to provide them with all necessary information, and management failed to do so, either purposely or negligently. Directors also relied on independent public accountants to detect illegal activity and to advise them of major risk exposures; unfortunately, the auditing procedures used by the independent accountants did not ensure that they could detect either illegal activity or major risk exposures.

WE WERE DUPED!

"We were duped!" is a common refrain by directors after every corporate scandal or financial disaster. For example:

- *Enron*. Sherron Watkins testified before Congress that the Enron board of directors was "duped." "As for the Enron board, some directors pointed fingers of blame at company management, especially [Andrew] Fastow [Enron chief financial officer]." One Enron director was quoted as saying "The board was duped." Herbert S. "Pug" Winokur, Jr., former head of the Finance Committee, testified that Enron was "a cautionary reminder of the limits of a director's role," which is by nature a "part-time job." He stated, "We cannot, I submit, be criticized for failing to address or remedy problems that have been concealed from us."

- *Tyco*. According to *USA Today*:

  > Tyco directors' lack of awareness and events surrounding criminal charges against CEO Dennis Kozlowski underscore the lax oversight of management that plagues many company boards, corporate governance experts say. . . . The head of The Directorship Group, a director search firm, stated: "Just how do you hide this much money for so long from your board? . . . It's their job as a director to know what's going on."

- *Merrill Lynch*. Stan O'Neal, the Merrill Lynch CEO prior to its forced merger with Bank of America, decided not to tell the board about an $8 billion write-down of its mortgage-backed securities. Other executives at the company were aware of its huge exposure to the subprime market and had warned O'Neal, but the board was in the dark allegedly because O'Neal did not initially believe the exposure was that large. According to the book *All The Devils Are Here*:

> The board members were stunned. Their anger turned to fury. Some began grilling O'Neal on Merrill's exposure; others complained that his approaching Wachovia [Bank, another suitor,] was a terrible breach of corporate etiquette—a CEO is supposed to get a board's permission before approaching another company. "Their reaction was vitriolic," recalls one participant. "I've never seen that kind of interplay between a CEO and a board of directors."

This huge exposure to the subprime mortgage market forced Merrill Lynch to disclose on October 24, 2007, a net loss of $7.9 billion on its collateralized debt obligations and resulted in its merger in late 2008 with Bank of America, N.A.

- *Lehman Brothers Holdings Inc*. According to the Bankruptcy Examiner's Report: "As their bad business decisions were pushing it toward collapse, top executives of the failed investment bank, Lehman Brothers Holding, Inc., repeatedly withheld information from their own board." The report states that in May 2008, a Lehman senior vice president, Matthew Lee, wrote a letter to management alleging accounting improprieties, asserting that Lehman used $50 billion of Repo 105 transactions (a questionable accounting technique) to temporarily move assets off balance sheet at quarter-end, but these allegations were never brought to the board's attention. According to the report: "Senior executives did not disclose to the board of directors at the September 9, 2008 finance committee meeting the fact that a substantial portion of its liquidity pool was encumbered by clearing-bank pledge." The report further states that "Lehman officers did not disclose to the board of directors that its liquidity position was substantially impaired by collateral held at clearing banks until the evening of September 14, 2008." The bankruptcy filing occurred on September 15, 2008.

The board of directors is required to oversee and monitor the activities of an organization's executive officers. If board members rely solely on information provided to them by the senior executives, they are risking their business reputations. For example, Herbert Winokur, Jr., an Enron director, was forced to step down from his position at the Harvard Corporation, the governing body of Harvard University, as a result of the Enron bankruptcy.

There have been numerous cases of CEOs and senior managers who lied on their resumes and subsequently were fired or disciplined. For example:

- On February 1, 2000, Jeffrey P. Papows quit as president of IBM's Lotus unit because of discrepancies in his education and military records.

- In October 2002, Kenneth Lonchar, the chief financial officer (CFO) of Veritas Software, was forced to resign after making false claims that he was a Stanford MBA graduate.

- In November 2002, Bausch & Lomb, the eye care company, announced that chairman and chief executive Ronald Zarrella would forfeit $1.1 million because his resume falsely noted an MBA from New York University.

- In November 2002, MSG Capital chairman and CEO Brian Mitchell admitted falsifying a degree from Syracuse University. Although he continued on as CEO, the stock price fell 37 percent after the announcement, hitting a 52-week low.

- In February 2006, the CEO of RadioShack Corp., David J. Edmondson, resigned following the revelation that he had lied on his resume about earning certain college degrees.

If some CEOs are willing to lie on their resumes, they also may be willing to lie to boards of directors. Accordingly, independent directors should not take as gospel anything that is said to them by the CEO or senior management.

EXECUTIVE WHISTLEBLOWERS

Lower-level executives typically are aware of potential scandals and major risk areas and bring these concerns to the attention of higher-level management. Higher-level management also may bring them to the attention of the CEO. The CEO, for one reason or another, may decide not to share these concerns with the board.

A major advantage of a robust whistleblower policy is to encourage greater communication of significant organizational risk exposures directly to the board of directors and particularly to the independent directors. Members of lower-level management often disagree with the CEO on risk exposures, but they have no opportunity to communicate their concerns directly to the board without fear of punishment by the CEO.

For example, prior to the collapse of AIG, certain executives recognized the major risks being undertaken through its derivatives business in credit default swaps but had no incentive to reveal these risks to the directors. According to an article by Michael Lewis, an author, in mid-2005, an AIG executive named Eugene Park was fiddling around at work with his online trading account after reading about this wonderful new stock called New Century Financial with a terrific dividend yield. Park looked at New Century's financial statements and noticed something "frightening." The average homeowner counted on to feed the interest on the A+ tranche of New Century mortgage-backed collateralized debt obligations (CDOs) had a credit score of only 598, with a 4.28 percent likelihood of being 60 days or more late on payment. Park subsequently discovered that the AIG Financial Products Division was insuring a substantial portion of the New Century mortgages. He allegedly revealed this information to Joseph Cassano's (the AIG executive in charge of swaps) number-two person in the AIG financial products division and ultimately was blown off. Had a robust whistleblower system existed at AIG at that time, Park might have used it to advise the AIG audit committee. Instead, the AIG financial products division did not reduce or hedge its existing supersenior tranches of subprime CDOs, although it stopped writing credit default swaps in late 2005–2006.

Likewise, some senior officers at Merrill Lynch recognized its major exposure to subprime mortgages well before its forced merger into Bank of America; their warnings were ignored by the CEO.

The Financial Crisis Inquiry Report notes that one of the two Bear Stearns executives stated in a diary in his personal e-mail account in 2006, long before the firm's collapse, that "a wave of fear set over [him]" when he realized that the Enhanced Fund "was going to subject investors to 'blow up risk'" and "we could not run the leverage as high as I had thought we could."

A robust whistleblower system, as discussed in the next chapter, would create incentives for people to report such significant risk information anonymously to independent directors, thereby alleviating fear of retaliation from the CEO. A robust whistleblower system that guarantees anonymity and offers meaningful rewards might induce lower-level executives to provide independent directors with the same information. Without those guarantees, no one is going to risk their career by going over the head of the CEO.

Some directors believe that they can speak privately to lower-level company executives and obtain truthful and accurate information, even if that information contradicts information that the CEO or CFO has supplied to the board. What these directors do not realize is that lower-level executives are generally unwilling to jeopardize their careers with the company by contradicting the CEO or CFO even in private conversations with directors. The disincentives to whistleblowing, discussed earlier, make it unlikely that lower-level executives will be candid with directors unless their identity is completely protected. Only a naive or a very brave executive would take the risk that his or her name would not ultimately be revealed to higher-level executives after private conversations with directors.

The Enron case provides an example of private conversations between a director and a lower-level executive that failed to reveal important information. Director Winokur claims to have had several private conversations with an Enron risk management executive well before any problems with the company surfaced. Winokur claimed that the executive never advised him of problems at Enron, but that same executive testified publicly after the Enron bankruptcy that he did not like some of the derivative hedges that Enron was using. Winokur should not have been surprised by the lack of candor of this risk management executive who would have risked his career by being candid with a director.

A robust whistleblower policy would have allowed the Enron executive to communicate with the independent directors in a manner that guaranteed anonymity. Although there is no assurance that this person would have used such a system, had it been available, the system would have provided the best chance for independent directors to obtain candid information from the executive ranks.

In summary, independent directors typically must rely on the CEO and CFO for almost all of their information about the company, subject to any additional information that they may receive from independent or internal auditors. It is difficult for independent directors to provide management oversight when most of their information comes from top management. This problem is exacerbated by the fact that a director's job is part time only and does not give him or her the necessary access to important corporate information.

Portions of Chapter 7 – Establishing a Robust Whistleblower System

THIS CHAPTER DESCRIBES a robust whistleblower system. Such a system should be adopted not only by public companies but by all organizations of any significant size, including not-for-profit organizations and government entities. Indeed, Internal Revenue Service (IRS) Form 990 (Part VI, Line 13) for tax-exempt organizations specifically asks whether the organization has a "written whistleblower policy." Even smaller organizations should adopt a robust whistleblower system, but they may tailor the system recommended in this chapter to their size.

The object of a robust whistleblower system is to encourage legitimate whistleblowers to provide valuable information to the board of directors (or other controlling group) of the organization, which is not being supplied to the directors by the chief executive officer (CEO) or chief financial officer (CFO) or through the internal auditor or the independent auditor. This information can help the organization prevent or cease illegal activities and identify major risks that it may incur. Whistleblower information permits the board of directors (or other controlling group) of an organization to more effectively fulfill their fiduciary obligations to the organization.

Many organizations, particularly public companies, have installed employee hotlines that are used only occasionally. Independent directors may incorrectly assume that the lack of employee hotline usage is an indication of a lack of illegal activity. That is not necessarily the case. As explained later in this chapter, the lack of hotline usage may merely indicate the lack of an effective whistleblower system, including the failure to provide incentives to employees sufficient to overcome the substantial disincentives of using the hotline and becoming known as a whistleblower.

A robust whistleblower system can encourage internal reporting of illegal activities or major risk exposures so that the problems can be corrected internally. Empirical studies have indicated that nearly all whistleblowers first report perceived wrongdoing to parties within their organizations. Unfortunately, too often these initial reports are ignored within the organization.

Equally important, a robust whistleblower system helps to prevent financial disasters where the board must claim that "we were duped" by the CEO or CFO. Director claims of being duped are not effective to prevent damage to their business reputations. More important, as noted in Chapter 6, such a system prevents criminal and civil liability of both the organization and its directors and officers.

As discussed, many boards of directors that relied solely on the CEO, CFO, and the internal and independent auditors for information have been misled. The history of scandals starting with Enron and ending with Lehman reveals that the board is often the last to know of the company's problems. The essential information that could have prevented these scandals was possessed by lowerlevel executives who had no incentive to go over the head of the CEO or CFO and "squeal" to the independent directors. A robust whistleblower system with independent directors in charge provides the best opportunity for the board to avoid unpleasant surprises.

An effective whistleblower system is really an internal control mechanism for accounting and auditing purposes. A whistleblower system should be considered an entity-level internal control, similar to the audit committee.

PROBLEMS WITH THE CURRENT WHISTLEBLOWER SYSTEM

Although Congress, when passing the Sarbanes-Oxley Act of 2002 (SOX), may have contemplated an active and effective whistleblower program, this goal has not been uniformly realized.

There are seven major problems with the current whistleblower systems:

1. The tone at the top tolerates but does not encourage whistleblowers.

2. There is no meaningful reward or recognition for legitimate whistleblowers.

3. The inability to communicate with anonymous whistleblowers results in failure to fully investigate anonymous information.

4. The system does not guarantee anonymity.

5. The system is not well advertised.

6. The audit committee uses employee administrators and investigators who are not viewed as independent by whistleblowers and who cannot use legal privileges to preserve confidentiality.

7. Whistleblowers' motivations and personalities affect the investigation.

Many public companies have a "paper" whistleblower system. In such a system, the company has complied with the letter of the SOX requirements and exchange listing rules but has done nothing more. Management tolerates the whistleblower system but does not encourage whistleblowers. Whistleblowers are almost never recognized as employees of the month. As a result, potential whistleblowers, facing daunting disincentives, refuse to participate in the system.

Concerning the SOX whistleblower statute, the former general counsel of the Securities and Exchange Commission (SEC) has stated:

> Not all corporate compliance programs work well. Some—no matter how elaborately conceived and extensively documented—exist only on paper. Some small number are shams. I once knew of an ostensibly anonymous employee hotline that actually rang on the desk of the CEO's secretary. I'm not at all sure that Congress intended that a whistleblower at this company would have to avail himself of this hotline before coming to the Commission and getting an award.

Very few, if any, whistleblower systems provide meaningful rewards or recognition for whistleblowers. Given the real possibility that the employment of persons disclosing wrongful activity may be terminated and even if not terminated such person could be socially ostracized,

employees have no reason to assume those risks without a meaningful incentive. Internal whistleblower systems do not have to compete economically with the size of awards available under the whistleblower statutes since there are many disincentives to employee whistleblowing, as detailed in Chapter 4. However, the lack of any meaningful reward or other recognition for whistleblowers reflects an organizational attitude that is not conducive to whistleblowing.

Although the SOX whistleblower system allows for anonymous whistleblowers, that system does not work well because the audit committee or its counsel may need to further question the person whose identity has been hidden. As discussed later in this chapter, the result is that audit committees tend to provide fewer resources to investigating anonymous complaints. Unfortunately, approximately half of whistleblower calls in 2009 were anonymous, a fact that suggests that many employees fear retaliation.

Moreover, some current whistleblower systems do not guarantee anonymity. Voice recognition techniques can be used to trace hotline calls. Private detectives can use handwriting analysis to trace anonymous letters. Anonymous e-mails can be traced back to the whistleblower's computer. The best practices described in this chapter provide greater guarantees of anonymity by permitting communication only through the whistleblower's personal counsel and permitting the whistleblower to form an entity to further hide his or her identity.

A study of fraud cases in large U.S. companies found that the percentage of employee whistleblowers dropped significantly after SOX compared to before SOX. It has been speculated that the job protection provisions of SOX were inadequate in light of the social ostracism and negative career impact on whistleblowers. This study emphasized the importance of both whistleblower anonymity and monetary rewards for whistleblowers.

Many companies do not adequately communicate the whistleblower system except in a policy contained in an SEC filing or on their websites. As a result, average employees may not realize that the company even has an anonymous whistleblower system. A survey by the Institute of Internal Auditors indicates that employee familiarity with the organization's hotline is a key factor in encouraging its use. The best practices described in this chapter provide for much better methods to communicate the whistleblower system to employees.

Investigations of whistleblower complaints are typically performed initially by the internal auditor, director of compliance, human resources (HR) head, or general counsel. All of these individuals are company employees whose compensation is determined by management (with the possible exception of the internal auditor). Potential whistleblowers do not have confidence in the independence or impartiality of these investigators. Moreover, many of these individuals are not skilled forensic investigators.

The best practices described in this chapter advise companies to use employees only to investigate lower-level complaints that do not involve executives (e.g., discrimination and sexual harassment complaints and reports of minor financial discrepancies) but use independent counsel (or other ombudsmen) to investigate all other complaints. Internal auditors remain the eyes and ears of the audit committee under a robust whistleblower system but will not investigate any whistleblower complaints, except for minor ones.

A key factor in employee willingness to use hotlines is the communication of the results of investigations of hotline tips and the actions taken. Many companies do not adequately communicate this information to the whistleblower.

Moreover, whistleblowers with difficult personalities or who have obviously ulterior motives may receive short shrift in any investigation, even though their complaints may be valid. SEC officials made this mistake in ignoring Harry Markopolos's revelations about Bernie Madoff approximately 10 years before his Ponzi scheme was revealed.

In summary, most current SOX whistleblower systems are not sufficiently robust to attract potential internal whistleblowers. Internal compliance systems do not have to compete monetarily with available statutory awards since most potential internal whistleblowers prefer not to suffer the disincentives of going public with their information, including waiting many years for any bounties from litigation. However, it is necessary for the SOX whistleblower systems to provide sufficient incentives to potential internal whistleblowers to induce them to provide to the organization the information necessary to correct law violations and to reveal significant risk exposures.

INITIAL STEPS

Two initial steps that should be taken in order to establish a robust whistleblower system are described next.

> **Best Practice**
>
> The company's employee booklet and any agreements signed by employees should include references to the company's zero-tolerance policy for violations of applicable law.

It is a no-brainer that the company's employee booklet should contain a reference to its zero-tolerance policy for law violations. However, a similar provision should be inserted in confidentiality agreements, invention disclosure agreements, and other agreements typically signed by employees in order to emphasize the importance of this policy to employees.

> **Best Practice**
>
> Employees at all levels should be required to report major risk exposures of the organization in addition to any potential law violations.

A robust whistleblower system should require employees at all levels to report law violations and major risk exposures of the organization. These reports may, at the employee's option, be provided anonymously. As discussed later, the reports should go directly to the independent directors or independent counsel (or an ombudsman).

It is important for the independent directors to obtain information about any major risk exposures of the organization. Senior executives may be aware of these risk exposures and may have reported them to the CEO or CFO only to have these officers ignore the warning. Normally senior executives are not willing to go over the head of the CEO or CFO directly to the board of

directors or the independent directors. Such actions would likely lead to very short careers and may even result in blacklisting in the industry. However, conscientious senior executives who are absolutely assured of anonymity may be willing to take that risk.

ELEMENTS OF A ROBUST WHISTLEBLOWER POLICY

An effective compliance program requires the following elements, each of which is discussed in this chapter:

- Independent directors must be in charge and must be given the resources to fulfill their responsibilities.
- The whistleblower system must be independently administered.
- Whistleblower complaints should be investigated by independent counsel (or other ombudsman) reporting directly to the independent directors.
- There should be no presumption that anonymous complaints are less deserving of investigation.
- The motivations and personality of the whistleblower are not relevant to the truth of the allegations.
- Absolute protection of whistleblowers' identity is essential.
- Periodically assess the effectiveness of any employee hotline and provide employee compliance training.
- Independent counsel should report to the whistleblower the status and results of the investigation and the organization should provide annual reports to all employees as to actions taken.
- Legitimate employee whistleblowers should receive meaningful monetary rewards.
- The whistleblower policy must be communicated effectively.
- There should be milder sanctions for whistleblowers involved in illegal group activity.
- Retaliation claims should be independently investigated.
- The director of corporate compliance (if any) should report to the independent directors and become their eyes and ears within the organization.
- The tone at the top of the organization must support an ethical, law-abiding culture. (See "Do's and Don'ts for CEOs" section below).