



## The Whistle

### Reducing the Risk of Whistleblower Complaints

**Whistleblowers** come in all stripes, from disgruntled present or former employees or customers to high-level executives trying to do what they see as the right thing. Sometimes their complaints have merit or at least partially so, and other times they are based on inappropriate or venal motives, exaggerating events or manipulating facts to the author's advantage. Whether they concern securities fraud, sexual harassment or other contentious areas, addressing whistleblower complaints has proven especially demanding for companies. Some laws mandate procedures to allow for these complaints, others require investigation of certain types of claims and still others protect the whistleblower from retaliation.

As this has become increasingly prevalent, best practices have emerged for how to handle the whistleblower, the substance of the complaints and the risks that go with them.

These range from establishing clear complaint channels, basic internal investigation procedures, and an investigatory team and plan, to developing appropriate educational and training programs for managers and compliance officers in this area. Executives need to be trained in how to deal with employees who make reports of possible wrongdoing and how to handle sensitive situations that might give rise to whistleblowing claims.

Minimizing the risk of liability from retaliation claims by alleged whistleblowers can be achieved by a proactive approach on the part of corporate management that anticipates the receipt of reports from actual or self-styled whistleblowers, establishes well-defined and well-publicized procedures for receiving and investigating such reports, identifies the appropriate corporate executives and advisors to evaluate the results of the investigation, determines whether and what corrective actions are necessary, and creates a protocol for protecting employee complainants and witnesses from possible retaliation.

#### Reporting Complaints

To encourage employees to report corporate fraud and other transgressions, federal and state statutes protect employees who raise concerns about various types of workplace misconduct.

For example, Sarbanes-Oxley requires publicly traded companies in the United States to implement policies and procedures for receiving reports from employees regarding "questionable accounting or auditing matters." Sarbanes-Oxley grants extensive protections to employees who report to their supervisors, Congress or any federal agency conduct that the employee reasonably believes violates certain federal fraud statutes, any SEC rule or any regulation concerning fraud against shareholders.

Substantial penalties may be imposed for violations of Sarbanes-Oxley's whistleblower protection rules, including reinstatement, backpay with interest, special damages, attorneys' fees and litigation costs, as well as criminal sanctions. Liability may be imposed not only for the actions of the company itself, but also for retaliatory acts by individual officers and employees, the company's contractors, subcontractors or other agents. Companies have established a variety of whistleblowing reporting mechanisms, including drop-boxes, hotlines and e-mail or web-based reporting vehicles, both anonymous or self-identified, and often administered by third-party service providers. Reporting categories, complaint tracking, responsible management recipients, other internal company routing, progress monitoring, investigative follow-up, case result and closure, and even relevant data archiving are part of current service provider offerings. These are all tailored to the corporation's particular selections and practices, both in the United States and in foreign countries. Ethics and compliance officers now routinely receive training on establishing, monitoring and executing whistleblower compliance programs.

#### Conducting the Investigation

Once a complaint is received and routed, the next stage is the internal investigation, its scope and the process surrounding it. A well-conducted investigation is an essential component of an employer's efforts to protect itself and its employees from the effects of purported wrongdoing by co-workers and third parties. Conversely, a flawed investigation may not only fail to achieve its protective purpose, but also impair the defense of the employer against claims by purported whistleblowers, government investigators or others.

The statutes that require employers to investigate allegations of employee misconduct do not dictate who should perform the investigation, what steps to take, how quickly to conduct and conclude the investigation, or what response is necessary or appropriate. These issues are left to the employer's discretion, which in turn allows the employer to tailor the investigation to the nature of the complaint and to adjust for other circumstances.

Certain core principles can guide the formulation of an effective investigation process. Elements to consider in designing and implementing an effective investigatory process include; *Timing, Consultation with counsel, Notification to the board of directors or the audit committee, Involvement of human resources, Creating an investigative plan, Interview preparation, Making and communicating a decision.*

#### Protecting Privacy

When a whistleblower complaint is made, the employer must be mindful of the need to minimize unnecessary disclosure to the workforce while actively investigating the employee's concerns in an expeditious and thorough manner. The employer cannot guarantee complete anonymity to the employee making the complaint (unless, of course, the complaint itself was made anonymously), or any other person interviewed as part of the investigation.

At the same time, the matter should be kept as confidential as possible and should not be disclosed beyond what is reasonably necessary. All witnesses should be advised to maintain appropriate confidentiality and not gossip or disclose questions asked of other co-workers. Of course, the employer should also make clear that it will not tolerate any retaliation against anyone who participates in the investigation. Logistical considerations for conducting interviews are equally important. This means careful practical arrangements and thought given to a number of basic items.



## The Whistle

### Reducing the Risk of Whistleblower Complaints

With the emergence of new rules about data protection in whistleblowing protocols, particularly in the European Union, employers face an even greater challenge in conducting lawful and effective investigations. In those countries, U.S. public companies are still required have to a Sarbanes-Oxley whistleblower program and code of ethics in place. However, the EU now has whistleblower guidelines and some countries, like France, have special online programs for whistleblower program approvals, which set detailed operating parameters.

EU data protection laws also put limits on internal disclosures of whistleblower complaints and mandate immediate disclosure of certain details of the complaint to the accused person, unless certain exceptions apply. The hotline report or investigation details, if containing personal information, cannot be transmitted to corporate headquarters in the United States without particular precautions, for example, consent of the individual(s), data protection agreements or enrollment in the U.S. Safe Harbor program.

Also under EU guidelines, once the complaint is lodged, the incriminated person is to be notified of the details, provided that the identity of the whistleblower must not be so disclosed. This notice to the accused can be delayed for evidence preservation purposes, such as backing up the computer, mirroring the hard drive or other procedures. This individual also has the right to correct or contest the data, if inaccurate, and has what are known as "access" rights to know what data is held about him or her in the process.

#### Preventive Measures

Because of the variety of state and federal statutes that protect potential whistleblowers, few corporations are free from liability for claims by employees who allege that they are victims of retaliation for whistleblowing. For global corporations, the liability risk is significantly greater in light of recent case law indicating that Sarbanes-Oxley's whistleblower protection provisions can reach across international boundaries.

To reduce the risk associated with whistleblower claims, companies should take the following preventive measures in addition to developing an effective process for receiving, investigating and evaluating whistleblower complaints:

- All subsidiaries, foreign and domestic, should have well-publicized and readily accessible policies and procedures for reporting corporate wrongdoing. Care should be taken to tailor the procedures to the requirements of foreign jurisdictions, particularly where those jurisdictions regulate or prohibit anonymous complaints.
- Complaint procedures should expressly prohibit retaliation against individuals who report possible wrongdoing. At the same time, separate procedures should be created for reporting retaliation complaints. The complaint procedure should specify the individuals to whom employees can report retaliation complaints and provide employees with alternative channels for reporting.
- Employers should develop training programs to educate officers, directors, managers and all other employees as to complaint policies and procedures, as well as the prohibitions against retaliation under Sarbanes-Oxley, and educate the personnel who handle these complaints to the possibility of extraterritorial applications of Sarbanes-Oxley and its regulations.
- Managers should focus on documenting performance deficiencies in the ordinary course of business so that a documented record exists prior to an employee's engaging in whistleblowing activity.

There is no "one size fits all" in handling whistleblower complaints, but following necessary precautions will help manage the complaint process and reduce the risks accordingly.

*Mark E. Schreiber and David R. Marshall are partners in the labor and employment group of the 500-attorney national law firm of Edwards Angell Palmer & Dodge. The authors would like to acknowledge the efforts of associate Robert Young who contributed to this article.*

*Parts of this article have been modified please refer to the following link for the complete article. <http://www.rmmagazine.com/Magazine/PrintTemplate.cfm?AID=3223>*

**Whistleblower Security Inc., is a 24/7 communications service that assists companies in their compliance requirements for Sarbanes Oxley and ML 52-110 and offers employees a confidential and anonymous method to report wrongdoing in the workplace through a proprietary software system and live contact centre.**

**FOR DETAILS OF HOW OUR UNIQUE WHISTLEBLOWER SECURITY SYSTEM CAN HELP YOU CONTACT 604.921.6875 OR EMAIL: [info@whistleblowersecurity.com](mailto:info@whistleblowersecurity.com). OR visit [www.whistleblowersecurity.com](http://www.whistleblowersecurity.com) For a DEMO today.**



## The Whistle

### Managing Corporate Thievery in the Age of Portable

It used to be that an employee desiring to steal \$2 million from your company would have a hard time doing so unnoticed. Today, that employee can do so undetected while having a casual conversation with you in the office.

Up until recently, sophisticated firewalls and password protection have been relatively sufficient to protect sensitive company information. Now, these measures are anything but sufficient. The proliferation of electronic devices such as iPods, camera cell phones, thumb drives, Blackberries, flash drives and all other sorts of downloadable devices have made all companies at risk for insider theft right under their proverbial noses. With the use of these devices, downloading significant amounts of data is easy, virtually instantaneous and often very difficult to detect.

Indeed, numerous companies have had valuable proprietary information stolen covertly by their own employees. Those that haven't yet are undoubtedly at risk. The security risks associated with these new portable electronic devices apply to essentially all companies that, in the course of doing business, allow employees' access to electronically stored, confidential and proprietary information.

#### THE UNIFORM TRADE SECRETS ACT

Unfortunately, in the current environment, the legal system is not forgiving toward companies that take a more relaxed approach with respect to protecting their own sensitive information. The Uniform Trade Secrets Act, adopted by many states, requires that companies exercise reasonable efforts to maintain the secrecy of confidential information before the information can be protected under trade secrets laws. A lack of such efforts taken by a company precludes its ability to seek protection of its sensitive information.

And although industry studies show that 70 percent of company computer system hackings are executed by company insiders, even when theft isn't a goal by insiders, the pocket devices used by employees to transport data between home and work, or on the road when traveling, are susceptible to theft just like any other piece of personal property. The person who happens to find the thumb drive inadvertently left behind in a cab can exploit the company information on the device just as easily, if not more easily, than the hacker that used to represent the company's biggest security concern.

Stolen private customer or client information not only puts a business and its trade secrets at risk, but also subjects the business to legal liability claims by individuals or other companies whose private information is leaked as a result. In addition, the business's reputation and ability to attract new customers or investors in the future may be damaged beyond repair.

So what is today's company supposed to do to protect its valuable, sensitive information in the face of the risks posed by new portable devices?

#### PREVENTING DOWNLOADING ABUSE

Of course, the most efficient way to prevent downloading abuse is to ban use of these portable electronic storage devices, a move that many companies have considered. Yet, the convenience and value to companies afforded by these devices is difficult, if not impossible, to ignore. The ability of employees to transport data so that they may work from anywhere provides enormous value to companies, sometimes affording them efficiencies not obtainable otherwise.

The ability to work outside the office gives companies a competitive advantage. It is often not only necessary for today's companies to remain competitive, but their clients also demand it.

While not foolproof, there are many other less dramatic changes a company can implement to protect itself from vulnerability while still enjoying the benefits of today's portable technology:

1) Adopt a policy forbidding misuse. Such a policy, often referred to as a "Portable Storage Device Policy,"; announces to employees, and ultimately to courts, that the company does not tolerate abuse of portable storage devices. The policy should include the following elements:

- a statement detailing the intent and purpose of the policy, i.e., why portable storage device usage is a concern and how the company is acting to address the risks associated with it;
- a nonexclusive list of the technologies and devices to which the policy applies, such as camera cell phones, PDAs, iPods and other devices for downloadable music, CD burners, thumb drives, etc.;
- a mandate forbidding personal storage devices from being attached to company computers or networks and requiring that only company-provided and approved portable storage devices may be used for data storage and transport;
- a requirement that passwords are to be activated on all possible devices and a description of any technical safeguards implemented in furtherance of that policy;
- a statement reminding employees about the risks of theft and imposing a reminder to exercise reasonable care to guard against it;
- a suggested point of contact for reporting concerns, including other employees' misuse of portable devices or theft of a device holding company information; and
- a general reference to the employer's other data policies and/or a section detailing procedures for data handling, including how and when portable storage usage is allowed (i.e., before attaching a portable storage device, the user must be identified and authenticated and a virus scan completed), as well as a requirement that all downloaded information must be encrypted.



## The Whistle

### Managing Corporate Thievery in the Age of Portable

The policy should be distributed to all employees and conspicuously posted. Ideally, it should contain a signature page requiring employees to read and sign off at the outset of employment.

It should also be easily accessible on the company intranet or other frequented place for information on employee policies. And, as with other important employee policies, it should be redistributed annually to employees and updated as needed to reflect the changing face of technology.

2) A company serious about protecting its information may also consider having employees complete cybersecurity and information privacy courses annually. Consistent with the underlying technology, these courses could be Internet-based training programs.

3) A company should consider employing an appropriate electronic device security system that requires authentication of users, records information about the devices attached to it and performs automatic virus scans. Such a system should also automatically encrypt all stored data at high speeds without requiring employees to do anything beyond authentication. Companies may also consider implementing security systems that allow network administrators to monitor and grant or deny access to employees attempting to download particular information with specific devices.

4) An employee exit interview is a company's last chance to protect its valuable information. Companies should require that all employees deliver back any computer, portable electronic storage device or other device upon which company information has been stored, before they leave the company's employ. Even employee-owned devices upon which company information has been stored should be brought in to be cleaned of any proprietary or sensitive company information before an employee leaves the company's employ (assuming the company allows these devices to be used).

Employees should be required to certify their compliance with these requirements. This provision may be included in the Portable Storage Device Policy agreed to by employees at the outset of their employment, and final paychecks may even be delayed until complied with, so long as the policy reflects such requirements and the withholding is consistent with state wage and hour laws.

#### CONCLUSION

Remember, even if not foolproof, these measures will at least assist a company in proving to a court that it used reasonable efforts to maintain the secrecy of its valuable information. Such a finding increases the company's chance of having its sensitive information protected by trade secret laws, allowing it to demand the return of such information and even sue for damages associated with its misappropriation.

It also will save the pain of having to explain to investors or customers why the company's sensitive information is available for public consumption, a prospect just as frightening as having trade secrets out in the open, vulnerable to the competition.

*Michael W. Droke, a partner at Dorsey & Whitney LLP, is the head of the Seattle office Labor & Employment Practice Group. Rachel E. Byrne is an associate in the group*

To remove your name from our mailing list, please reply to this email with "UNSUBSCRIBE" in the subject box.

Questions or comments? E-mail us at [Jatinder@whistleblowersecurity.com](mailto:Jatinder@whistleblowersecurity.com)