THE NATIONAL
LAW JOURNAL
WWW.NLJ.COM THE WEEKLY NEWSPAPER FOR THE LEGAL PROFESSION MONDAY, MAY 23, 2005 ALM

CONFIDENTIAL DATA

Mandatory Protection

By Nick Akerman

AS OF OCT. 31, 2004, companies listed on the New York Stock Exchange (NYSE) are required to be in compliance with the NYSE's corporate governance rules promulgated pursuant to the Sarbanes-Oxley Act. While § 406 of Sarbanes-Oxley only requires public companies to adopt codes of conduct governing "senior financial officers, applicable to its principal financial officer and comptroller or principal accounting officer," the code of conduct required by the NYSE is not so narrowly limited. Codes of conduct promulgated by NYSE-listed companies must apply to "directors, officers and employees," not just those involved in financial reporting, and must "address" conduct beyond financial reporting. NYSE's Listed Company Manual, § 303A, ¶ 10.

While recognizing that "[e]ach company may determine its own policies," the NYSE now requires a listed company to address confidentiality as a goal of its compliance program and to adopt a policy that its "[e]mployees, officers and directors should maintain the confidentiality of information entrusted to them by the company or its customers." Id. at 303A, ¶ 10. The NYSE rules broadly define confidential information to include "all non-public information that might be of use to competitors, or harmful to the company or its customers, if disclosed." Id. "Each code of business conduct and ethics must also contain compliance standards and procedures that will facilitate the effective operation of the code." Id. This includes providing "mechanisms to report unethical conduct."

The rules also provide that the chief executive officer of each NYSE-listed company "must certify to the NYSE each year that he or she is not aware of any violation by the company of NYSE corporate governance listing standards, qualifying the certification to the extent necessary." Id. at 303A.12. This article will examine how this rule requiring the protection of confidential information comports with trade secret law, the basis for the NYSE rule and what issues should be addressed in corporate codes of conduct to protect confidential information.

Trend toward mandatory protection of data

This rule places the NYSE at the forefront of a trend that is drastically changing the traditional rules on protecting a company's confidential information. It used to be that a company had the option of whether to protect its confidential information—an option that was driven solely by market incentives to keep the information away from the competition. Indeed, the courts will only protect company confidential information as a trade secret if the company itself takes reasonable steps to protect it. See, e.g., *Teleflora LLC v. Florists' Transworld Delivery Inc.*, No. C 03-05858, 2004 WL 1844847, at *6 (N.D. Calif. Oct. 5, 2004). The courts, of course, have never mandated that such reasonable steps be taken or that confidential company information be protected.

For NYSE-listed companies, taking reasonable steps to protect confidential information—whether it is their own confidential business information or customers' personal information—is no longer optional. Section 303A is part of a growing trend of laws and regulations requiring companies to protect confidential information. It started with privacy concerns over customer information in the financial services and health care industries. The Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 261-264, controls the use and acquisition of an individual's health information, and the Gramm-Leach-Bliley Act of 1998, 15 U.S.C. 6801(a), mandates "that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."

Protecting nonpublic personal information of customers in general has taken on a new urgency with the increase in identity theft. By obtaining an individual's personal information such as a Social Security number or credit card information, the identity thief can access the victim's bank accounts and buy merchandise with the victim's credit cards. In response to this problem, California passed an identity-theft statute, which became effective in July 2003 and requires any business located or doing business in California to notify customers if

Nick Akerman *is a partner in the New York office of Dorsey & Whitney.*

it has reason to believe that their personal information maintained in a computer database has been accessed without authorization. Calif. Civ. Code § 1798.82(b), et. seq.

Individuals who are later victimized by identity thieves and are not properly notified are entitled under the statute to sue for compensatory and punitive damages. The recent publicity surrounding the thefts of personal data from major companies such as ChoicePoint and LexisNexis will likely result in the enactment on both the state and federal level of even more stringent controls and penalties to protect personal customer information. The NYSE rule, requiring its listed members to protect "non-public information that might be...harmful to its customers, if disclosed," is part of this national trend.

The legal basis for protecting "all non-public information that might be of use to competitors, or harmful to the company...if disclosed," while a worthy goal, is less clear. This requirement is predicated on Sarbanes-Oxley's mandate, under §§ 404 and 302, that management establish and maintain "an adequate internal control structure and procedures for financial reporting," and that "the principal executive officer" and the "principal financial officer" "are responsible for establishing and maintaining internal controls" and must certify "the effectiveness of their internal controls." These provisions arguably require a public company to identify and value its confidential and proprietary information so it can determine which of these assets are material, require disclosure to investors and must be protected to preserve shareholder value.

Requiring a company to protect its confidential information that gives it a competitive advantage is a radical new approach. Neither the SEC nor any court have interpreted Sarbanes-Oxley to require the protection of intellectual property. Nonetheless, there can be little doubt that safeguarding a company's confidential information that could be of use to a competitor protects shareholder value in the company and is a corporate asset that can be protected through a corporate compliance program.

A code of conduct performs three functions. First, it mandates the obligations of all officers and employees to protect confidential information and defines the scope of confidential information belonging to the company. See, e.g., *Pickering v. American Express Travel Related Services Co. Inc.*, No. 98 Civ. 8998, 2001 WL 753782, at *7 (S.D.N.Y. July 2, 2001). Second, it establishes the rules for how officers and employees are to use the company's confidential information, e.g., who has access to sensitive documents, and whether they can be removed from the workplace.

For NYSE-listed companies, taking reasonable steps to protect confidential information—theirs or customers'—is no longer optional.

Third, it sets the predicate for being able to protect the company's confidential information through the courts. As mentioned above, it is part of the reasonable steps to protect information that are an element of qualifying the confidential information as a trade secret. The code of conduct can establish who is authorized to access and use company computer data—the key element in bringing an action against a thief of computer information under the Computer Fraud and Abuse Act. 18 U.S.C. 1030, et. seq.

Ensuring compliance with NYSE governance rules

The NYSE governance rules also require compliance standards and procedures that will facilitate the effective operation of the code. This means companies must adopt compliance programs akin to what is required under the Federal Sentencing Guidelines. A company does not fulfill its responsibilities by simply publishing a code of conduct. Rather, it must ensure that everyone understands the code's rules. This means not only acknowledging that one understands the obligation imposed by the code by signing a form (see, e.g., *Dresser-Rand Co. v. Virtual Automation*, 361 F.3d 831, 844 (5th Cir. 2004)), but also providing companywide training; high-level corporate oversight of the program; adequate funding of the program; mechanisms for reporting violations and responding to employee questions; and the capability to investigate potential violations. It also means taking appropriate remedial action when violations are discovered—which includes being prepared to file lawsuits to retrieve and halt the dissemination of valuable company information—and periodic auditing of the program to ensure its effectiveness.

Since most of a company's confidential information, whether its own information or customer information, is maintained as data in computers, particular emphasis should be placed on protecting the company's computer network. Thus, the code of conduct must address a myriad of computer issues such as e-mail policies—whether work can be sent home or confidential information can be sent over the Internet—and how employees can work with data—whether data can be copied to disks or universal serial bus sticks; whether personal computers can be used for company work; and protocols for returning computer data when an employee terminates employment with the company.

Equally significant is using technology to protect computer data. Beyond using passwords and firewalls, third-party software is available that will allow a company to delineate who is permitted access to a particular document on a "need to know" basis, to encrypt it when the document leaves the workplace and to maintain an audit trail of the document that provides admissible evidence that can be used in a court of law to prove the theft and the identity of the thief. Thus, rather than companies simply reacting to the theft of their confidential information, the NYSE governance rules require listed companies, prior to being victimized by a single theft, to take aggressive and proactive steps to protect their confidential information. NLJ

This article is reprinted with permission from the May 23, 2005 edition of THE NATIONAL LAW JOURNAL. © 2005 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information contact, American Lawyer Media, Reprint Department at 800-888-8300 x6111. #005-05-05-0030