

Disclosing Information Security Breaches Under Privacy and Securities Laws

By **Melissa J. Krasnow**

[Editor's Note: This is the second in a series of articles addressing some of the key issues surrounding corporate responsibility with respect to the privacy of information and security breaches.]

The Privacy Rights Clearinghouse estimates that over 100 million records containing sensitive personal information have been involved in security breaches. This non-profit consumer organization has tracked these breaches on its website (www.privacyrights.org) beginning with the significant and well-publicized ChoicePoint breach in February 2005. As a result, over two-thirds of states enacted security breach notification laws governing the notification that a company must make in the event of a security breach. This article outlines the requirements for providing notification of a security breach under state security breach notification law by any company and the factors that a public company needs to take into account regarding whether to disclose a security breach under federal securities law.

STATE SECURITY BREACH NOTIFICATION LAW

The following 34 states enacted security breach notification laws: Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio,

Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington and Wisconsin. In addition, Michigan passed such a law with an effective date of July 2, 2007. It is important to note that Congress is considering federal security breach notification legislation and it is anticipated that a federal security breach notification law will be enacted in the coming years. But until a federal law is enacted that preempts the state notification breach laws, compliance with the various applicable state laws is required.

California was the first state to enact a security breach notification law. The California Security Breach Information Act (S.B. 1386) became effective July 1, 2003. Since the California law serves as a model for a number of the other state laws, this article discusses the California law. In practice, it is necessary to refer to all state laws that are applicable to a specific situation.

APPLICATION

The California law applies to a company that does business in California and owns or licenses computerized data that contains personal information. A company could be deemed to be doing business in California merely by maintaining personal information about a California resident. Also, a company could own or license computerized data containing personal information that is physically located outside of California but still be subject to the California law.

DEFINITION OF PERSONAL INFORMATION

Personal information means an individual's first name or first initial and last name in combination with any of the following data elements, when either the name or data ele-

ments are not encrypted: 1) Social Security Number; 2) driver's license number or state identification card number; or 3) account number, credit card number or debit card number in combination with any required security code, access code or password (e.g., a PIN) that would permit access to an individual's financial account. But publicly available information that is lawfully made available to the general public from federal, state or local government records does not constitute personal information. It is important to note that this definition is substantially simi-

In last month's installment of this series, "Where Privacy and Corporate Governance Laws Meet: Information Security Obligations," the author described the *In re Caremark* litigation. It should be noted that in late 2006, in *Stone v. Ritter*, 911 A.2d 362 (Del. 2006), the Delaware Supreme Court held that *In re Caremark* stated "... the necessary conditions predicate for director oversight liability: (a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, [the directors] consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention." Where failure of this nature demonstrates "... a conscious disregard for their responsibilities, they breach their duty of loyalty by failing to discharge [their] fiduciary obligation in good faith.

Melissa J. Krasnow is a partner in the Corporate Group of Dorsey & Whitney LLP (e-mail: krasnow.melissa@dorsey.com).

lar to the definition of personal information under the California security procedures law. The difference is that medical information is not included under the definition of personal information.

DEFINITION OF SECURITY BREACH

A security breach refers to the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the company. However, a good-faith acquisition of personal information by an employee or agent of the company for its purpose if the personal information is not used or subject to further unauthorized disclosure is not a security breach.

NOTIFICATION OF SECURITY BREACH

Following the discovery or notification of a security breach, the company must disclose the security breach to any California resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Moreover, a company that maintains computerized data that includes personal information that it does not own needs to notify the owner or licensee of the information of any security breach immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person. Notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Notification can be provided in any of the following ways: 1) written notice; 2) electronic notice in compliance with the provisions of the Electronic Signatures in Global and National Commerce Act (E-SIGN); or 3) substitute notice, if the company demonstrates that: (a) the cost of providing notice would exceed \$250,000; (b) the affected class of subject persons to be notified exceeds 500,000; or (c) the entity does not have sufficient contact information. Substitute notice must consist of all of the following: 1) e-mail notice when the company has an e-mail address for the subject person or business; 2) conspicuous posting of the notice on the Web site

page of the business; and 3) notification to major statewide media.

Alternatively, a company that maintains its own notification procedures as part of an information security policy for the treatment of personal information and which is otherwise consistent with the timing requirements described above is compliant if it notifies subject persons in accordance with its policies in the event of a security breach.

FEDERAL SECURITIES LAW

A public company must consider whether to disclose a security breach in its reports with the Securities and Exchange Commission (SEC). While there is no specific obligation to disclose a security breach under federal securities law, there are reasons for doing so and there is precedent.

SECURITIES EXCHANGE ACT OF 1934

The disclosure controls and procedures of a public company must be designed to ensure that information required to be disclosed by the public company in its SEC reports under the Securities Exchange Act of 1934 (1934 Act) is accumulated and communicated to its management, including its Chief Executive Officer and its Chief Financial Officer, to allow for timely decisions regarding required disclosure. Disclosure controls and procedures means controls and other procedures that are designed to ensure that information required to be disclosed by the public company in its SEC reports is recorded, processed, summarized and reported within the requisite time periods.

A public company files periodic and current reports with the SEC to provide material information about the public company. Material information is information that a reasonable investor would consider important in making an investment decision. Additional considerations concerning the disclosure of a security breach include regulatory requirements and public relations.

A prominent example of the disclosure of a security breach in SEC reports is ChoicePoint, regarding the above-referenced breach that was made in a current report on Form 8-K under the heading for information that is not specifically required to be

disclosed but that the public company deems to be of importance to security holders. ChoicePoint also disclosed in this current report that it was the subject of inquiries by various regulators, including the SEC, the Federal Trade Commission and state attorneys general. Subsequent disclosures about this matter were made by ChoicePoint in its periodic and current reports.

It is interesting to note that the SEC inquiry related to trading in ChoicePoint stock by the Chief Executive Officer and the Chief Operating Officer. The 1934 Act and the rules promulgated thereunder and the insider trading policy of a public company prohibit trading by officers and directors in the stock of a public company on the basis of material nonpublic information. A security breach before disclosure could constitute material nonpublic information.

STOCK EXCHANGE RULES

In addition to its SEC reporting considerations, a public company must take into account the stock exchange rules regarding the disclosure of material news (e.g., New York Stock Exchange and NASDAQ), if applicable.

CONCLUSION

Disclosures about security breaches are becoming more numerous resulting in part from the recent enactment of various state security breach notification laws. As more public companies suffer security breaches and are required to make these notifications, they will need to consider whether to make disclosures in their SEC reports and comply with federal securities law and any applicable stock exchange rules. Accordingly, a public company should make sure that its privacy and securities law compliance procedures and practices are consistent.

