

## Where Privacy and Corporate Governance Laws Meet *Information Security Obligations*

By **Melissa J. Krasnow**

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

As business information, particularly in electronic format, continues to proliferate, the need to maintain the security of this information is increasing. There are privacy and corporate governance laws that govern the obligation of a company to keep information secure. According to the Global State of Information Security 2006, a worldwide study by CIO magazine, CSO magazine and PricewaterhouseCoopers representing the responses of almost 7800 senior executives, "Noncompliance runs broad and deep in all industries, and ignorance of applicable law is a big factor." This article provides an overview of two important information security obligations — security procedures and practices and document destruction — under privacy and corporate governance laws.

### **SECURITY PROCEDURES AND PRACTICES** *State Security Procedures and Practices Laws*

A few states have enacted laws regarding a company's duty to maintain reasonable security procedures and practices. Arkansas, California, Nevada, Rhode Island, and Texas and Utah enacted security procedures and practices laws. California was the first state to enact a security procedures law. Under the California law, a company that owns or licenses personal information about a

California resident must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification or disclosure.

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 elements are not encrypted: 1) Social Security number; 2) driver's license number or state identification card number; 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 or (iv) medical information.

### **Federal Trade Commission Security Procedures Standards**

Although there is no specific federal security procedures law for all companies, the Federal Trade Commission has described standards for security procedures in a number of recent cases. By way of example, in the BJ's Wholesale Club case in 2005, the FTC charged that BJ's failure to provide reasonable security for sensitive customer information was an unfair act or practice in violation of Section 5 of the Federal Trade Commission Act because it caused substantial injury that was not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition. The FTC alleged that BJ's: 1) failed to encrypt consumer information when it was transmitted or stored; 2) stored the information longer than it had a need to do so; 3) stored the information in files that could be accessed using commonly known default user IDs and passwords; 4) failed to use readily available security measures to prevent unauthorized wireless

connections to its networks; and 5) failed to use measures sufficient to detect unauthorized access to the networks. The settlement order for this case requires BJ's to establish and maintain a comprehensive information security program that includes administrative, technical and physical safeguards and to obtain regular third party professional audits of this program for compliance with the FTC Order and with book-keeping and record-keeping requirements. The FTC Order is in effect for a 20-year period.

### **Sarbanes-Oxley Act**

Pursuant to Section 404 of the Sarbanes-Oxley Act of 2002 (SOX), management of a public company is responsible for establishing and maintaining adequate internal control over its financial reporting. Management must evaluate and report on the effectiveness of internal control over financial reporting in the annual report filed by a public company with the Securities and Exchange Commission. This management report is accompanied by an attestation from the independent auditor of the public company. Management also must evaluate and disclose changes that have materially affected or are reasonably likely to materially affect a public company's internal control over financial reporting in the quarterly and annual reports. Moreover, the Chief Executive Officer and Chief Financial Officer of a public company must provide certifications regarding their responsibility for establishing and maintaining internal control over financial reporting and the design of internal control over financial reporting to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. These certifications are attached as exhibits to a public company's quarterly and annual reports.

---

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

### ***In re Caremark***

This suit against the board of directors of Caremark International Inc. involved claims that the directors breached their fiduciary duty of care to the company in connection with alleged violations by Caremark employees of state and federal laws. *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del.Ch. 1996). The plaintiffs sought to recover losses on behalf of the company from the directors. According to the Delaware Chancery Court:

[I]t is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility . . . [A] director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.

### **DOCUMENT DESTRUCTION**

#### ***State Document Destruction Laws***

Close to one-third of states have enacted laws requiring the destruction of documents. Arkansas, California, Hawaii, Indiana, Kansas, Kentucky, Montana, Nevada, New Jersey, North Carolina, Rhode Island, Tennessee, Texas, Utah, Vermont and Washington enacted document destruction laws. Under the California law, a company must take all reasonable steps to destroy or arrange for the destruction of the records of a customer within its custody or control containing personal information which is no longer to be retained by: 1) shredding, 2) erasing, or 3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

Personal information means any information that identifies, relates to, describes or is capable of being associated with, a particular individual, including: 1) name; 2) signature; 3) Social Security number; 4) physical characteristics or description; 5) address; 6) telephone

number; 7) passport number; 8) driver's license or state identification card number; 9) insurance policy number; 10) education; 11) employment; 12) employment history; 13) bank account number; 14) credit card number; 15) debit card number or 16) any other financial information. "Records" refers to any material regardless of the physical form on which information is recorded or preserved by any means (e.g., in written or spoken words, graphically depicted, printed or electromagnetically transmitted).

#### ***Fair and Accurate Credit Transactions Act***

The Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 (FACTA) requires a company that maintains or otherwise possesses consumer information for a business purpose to properly dispose of consumer information by taking reasonable measures to protect against unauthorized acquisition or use of the information in connection with its disposal. Consumer information means any record about an individual in paper, electronic or other form that is derived from a consumer report or a compilation of such record. Disposal refers to the discarding or abandonment of consumer information or the sale, donation or transfer of any medium (including computer equipment) upon which consumer information is stored.

Reasonable measures include establishing and complying with policies to: 1) burn, pulverize or shred papers containing consumer report information so that the information cannot be read or reconstructed; 2) destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed; and 3) conduct due diligence and hire a document destruction contractor or dispose of material specifically identified as consumer report information. Although the FACTA Disposal Rule applies to consumer reports and the information derived therefrom, the FTC, which enforces this Rule, encourages those that dispose of any records containing a consumer's personal or financial information to take similar protective measures.

#### **SOX**

Two sections under SOX that cover document destruction apply to a company, whether public or private. Section 802 of the Sarbanes-Oxley Act states:

[W]hoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record,

document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined ... imprisoned not more than 20 years, or both.

Section 1102 of SOX states in pertinent part:

[W]hoever corruptly ... alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or ... otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so ... shall be fined ... or imprisoned not more than 20 years, or both.

### **CONCLUSION**

As information security obligations are continually changing, the laws governing information security obligations are evolving. Laws in different areas like privacy and corporate governance are both addressing these obligations. As a result, a company must carefully and constantly monitor developments in all of these laws in order to comply with them. According to the Ernst & Young 2006 Global Information Security Survey, compliance requirements in the past year have most significantly impacted and in the next year likely will continue to significantly impact the information security practices of companies.

*Next month, the author will outline 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.*



This article is reprinted with permission from the February 2007 edition of the LAW JOURNAL NEWSLETTERS - THE CORPORATE COUNSELOR. © 2007 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM Reprint Department at 800-888-8300 x6111 or visit [www.almreprints.com](http://www.almreprints.com). #055/081-02-07-0004