THE NATIONAL
LAW JOURNAL
DAILY UPDATES ON WWW.NLJ.COM NEWS FOR THE PROFESSION MONDAY, MARCH 9, 2009
An incisivemedia publication

BUSINESS INFORMATION

State Compliance Laws

By Nick Akerman and Melissa J. Krasnow

Connecticut, Massachusetts and Nevada recently enacted laws requiring businesses to institute certain compliance measures to secure personal information that can be used to perpetrate identity theft. The Massachusetts law applies to a business located anywhere in the United States that stores or maintains personal information about a Massachusetts resident. This article discusses the requirements of these new state laws and their practical significance for businesses.

The personal information at issue includes Social Security, driver's license and financial account numbers, each in combination with a person's name. Forty-four states, including Connecticut, Massachusetts and Nevada, currently require businesses to notify individuals if there is a breach of personal information. This notification permits individuals to take steps to protect their credit cards and bank accounts from identity theft. Rather than simply requiring businesses to respond to a data breach with notifications, the new Connecticut, Massachusetts and Nevada laws impose certain compliance obligations on businesses to protect personal information from a data breach.

The Nevada and Connecticut laws each became effective on Oct. 1, 2008. The Nevada law, the least onerous of the three, mandates that "[a] business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission." Nev. Rev. Stat. § 597.970(1). Connecticut's security measures go beyond encryption. Businesses must "safeguard the data, computer files and documents containing the information from misuse by third parties" and "destroy, erase or make unreadable such data, computer files and documents prior to disposal." Conn. Pub. Act 08-16, § 1.

The Massachusetts regulation will require businesses storing residents' information to set up data compliance programs.

In particular, the Connecticut law focuses on Social Security numbers and requires businesses to "create a privacy protection policy which shall be published or publicly displayed...on an Internet web page" to "[p]rotect the confidentiality of...prohibit unlawful disclosure of...and limit access to Social Security numbers." Conn. Pub. Act 08-167. There is a civil penalty of $500 for each intentional violation, up to a maximum of $500,000 "for any single event." Id.

Massachusetts' regulation is the most comprehensive

A first-of-its-kind Massachusetts re–gulation issued by the state Office of Consumer Affairs and Business Regulation is the most comprehensive of the new laws. Businesses that own, license, store or maintain personal information about a Massachusetts resident must be in full compliance with this regulation on or before Jan. 1, 2010, including implementing a comprehensive, written information security program for personal information. 201 Mass. Code Regs. 201, 17.03-17.05. The Massachusetts attorney general is responsible for its enforcement.

This regulation in effect mandates businesses to establish a data compliance program that is consistent with the requirements of the Federal Sentencing

Nick Akerman *is a partner in the New York office of Dorsey & Whitney who specializes in the protection of trade secrets and computer data.* **Melissa J. Krasnow** *is a partner in the firm's Minneapolis office who focuses on privacy and security issues.*

Guidelines. U.S. Sentencing Commission, Guidelines Manual, § 8B2.1 (November 2004). This regulation recognizes that the program must be tailored to each business based on the size, scope and type of business; the amount of resources available to the business; the amount of stored data maintained by the business; and the need for security and confidentiality of both consumer and employee information. 201 Mass. Code Regs. 17.03. Like the Federal Sentencing Guidelines, the program must address the following seven issues:

1. *Develop security policies*. Initially, businesses must identify the personal information they have and develop employee security policies that limit the amount of personal information collected and the time it is retained as well as restrict physical access to that information to those with a need to use it. These policies must also be enforced through technology that, at a minimum, secures user-authentication protocols; has secure access control measures; to the extent technically feasible, encrypts all transmitted records and files containing personal information that will travel across public networks, and all data to be transmitted wirelessly; has reasonable monitoring of systems for unauthorized use of, or access to, personal information; encrypts all personal information stored on laptops or other portable devices; has reasonably up-to-date firewalls and operating system security patches for files with personal information on a system connected to the Internet, reasonably designed to maintain the integrity of the information; and has reasonably up-to-date versions of system security agent software.

2. *Appoint a security coordinator*. One or more employees must be designated to manage the program.

3. *Minimize risk with third parties*. Care must be taken to ensure that those who might misuse personal information, such as terminated employees, do not have access to the data. Also, businesses must verify that third-party service providers with access to personal information have the capacity to protect this information in the manner provided for in this regulation and ensure that these service providers are applying security protective measures at least as stringent as those required to be applied to personal information under this regulation.

4. *Train the work force*. Businesses must educate and train employees on the proper use of the computer security system and the importance of personal information security.

5. *Conduct regular audits*. At least annually, businesses must monitor the program and identify and assess risks to the security, confidentiality or integrity of records with personal information and evaluate the effectiveness of the current safeguards.

6. *Enforce the policies*. Businesses must impose disciplinary measures for violations and document responsive actions when a data security breach occurs.

7. *Respond to incidents*. Businesses must encourage employees to report violations and document responsive actions when a data security breach occurs.

These three new state laws augur what may be the start of a trend away from passive state regulation of personal information requiring a reactive approach when data are breached to stricter requirements aimed at protecting the data in the first instance. Previously, many states attempted to motivate businesses through their notification laws to encrypt or redact personal information to avoid the notification requirement in the event of a data breach. See, e.g., Kansas Stat. Ch. 50-7a01(h). In the future, more states are likely to require businesses to implement data security programs with varying degrees of complexity. Legislation is pending in Michigan and Washington to require businesses to encrypt stored personal data in accordance with accepted industry standards. A violation under the Michigan bill would be a misdemeanor with a 30-day maximum prison sentence and a $1,000 fine. Michigan Senate Bill No. 1022.

This trend toward proactive protection is evident in the federal system. Federal law requires financial institutions, 15 U.S.C. 6801 et seq., and health care providers, 42 U.S.C., 1320d et seq., to protect personal information. The Federal Trade Commission has responded to major data breaches by BJ's Wholesale Club Inc. and DSW Inc. with enforcement actions requiring the establishment of comprehensive data security programs. By May 1, under the FTC's "Red Flag" rules, financial institutions and creditors are required to conduct risk assessments and promulgate written programs designed to reduce and prevent identity theft. 16 C.F.R. pt. 681 appx. In the private sector, the New York Stock Exchange requires its listed companies to establish a data compliance program to protect "all non-public information that might be of use to competitors, or harmful to [a business] or its customers, if disclosed." NYSE's Listed Company Manual, § 303A.10.

Adopting a comprehensive data compliance program

The message is clear. The way to ensure compliance with all of the existing and likely future state and federal regulation of personal data and to minimize the chance of being penalized is to adopt a comprehensive data compliance program. There are several obvious advantages to having such a program. First, it will help minimize costly data breaches. Often, one breach affects hundreds of thousands of individuals.

Second, if a suspected data breach does occur (since there is no foolproof means to prevent a data breach), a data compliance program provides the in-place mechanism and protocols to respond immediately to determine whether notifications have to be made to law enforcement or individuals and do whatever else is necessary to demonstrate to the authorities and the public that the business is acting responsibly.

Third, a data protection program for not much extra cost can include the protection of a business' competitively sensitive data. Given the economic crisis and the increase in company downsizing, competitively valuable data is more vulnerable than ever to employee theft. There is a concern that "mass layoffs will incite a percentage of previously loyal employees to look at criminal activity" and "steal vital information" to start their own competing businesses or "to improve their job opportunities with the competition." McAfee Inc., "Unsecured Economies: Protecting Vital Information," February 2009 at 9-10, http://cicentre.com/reports/Unsecured_Economies_012909.pdf. NLJ