SEYFARTH SHAW LLP
ATTORNEYS

One Minute Memo®

Proposed Regulations Would Impact All Businesses With Personal Data On Massachusetts Residents

You may already know that Massachusetts recently joined 38 other states by enacting a data protection law which governs the security and disposal of "personal information" of Massachusetts residents. The first stage of this law, Chapter 93H, became effective on October 31, 2007 and requires notification to residents and state authorities if personal information (*e.g.* name and a personally identifiable number such as a credit card number or social security number) is improperly accessed or used. The second component of the law, Chapter 93I, mandates destruction of hard copy and electronic data containing personal information of Massachusetts residents and will become effective on February 3, 2008. This law impacts any company that collects, maintains, or owns personal information data on Massachusetts residents without regard to the location of the company's place of business.

While this law is modeled after other state data security statutes, the Massachusetts act imposes more significant burdens which previously have been imposed in other jurisdictions. For example, Massachusetts 1) requires companies and employers to send notifications of data security breaches concerning personal information in both electronic and hard copy (not just electronic form as most state laws require), 2) has a broader set of triggering events that require notices to be sent, and 3) notices have to be sent to the Massachusetts residents, as well as two state authorities. It also has stringent requirements for the destruction of personal data.

What you *may not know,* and what may be of more concern, is that proposed regulations drafted by the Massachusetts Office of Consumer Affairs and Business Regulations would have a dramatic impact on information security practice, company HR policies, and training obligations, essentially codifying certain security practices as law. Comments to these proposed regulations are due to the Massachusetts Attorney General and Office of Consumer Protection and Business Regulation on Friday January 25, 2008. Companies would be required to, among other things:

1) Implement a comprehensive information security program, including internal policies and procedures on the handling of personal information

2) Designate an employee in charge of security

3) Conduct an internal and external risk assessment relating to the collection, storage, and use of personal data held by the company

4) Implement and monitor employee data security training

5) Monitor employee compliance with policies and procedures

6) Analyze and upgrade, if necessary, computer/ information systems

7) Develop a telecommuting policy pertaining to data access and storage

8) Impose disciplinary measures for violations of program rules

9) Prevent terminated employees from accessing records

10) Take reasonable steps to verify that service providers treat data appropriately, including doing security due diligence, and obtaining written certification that the service provider has a written security program

11) Collecting, using and retaining personal information for the minimum necessary legitimate business purpose

12) Inventory records containing personal information

13) Regularly monitor and auditing employee access to personal information to prevent unauthorized use and access

14) Conduct at least an annual review of security issues or if there are material changes in business practices

15) Document all actions relating to security breaches

16) Implement specific computer system security requirements, including user authentication controls, access controls, encryption, monitoring, audit trails, firewalls, security agent, and antivirus software

17) Educate and train on proper use of the computer security system

18) Prepare written procedures restricting physical access to personal information

19) Implement mandatory review of the integrity of computer records when there is an unauthorized entry into a secure area

Although many companies may already voluntarily comply with many or all of these provisions, there is a difference between voluntarily implementing security practices and being legally mandated to do so. A copy of the proposed regulations can be reviewed by clicking here.

If you have any questions regarding this One Minute Memo, the law or proposed regulations, or if you may be interested in submitting comments to the regulations, please contact the Seyfarth Shaw attorney with whom you work, or any attorney on our website, www.seyfarth.com.