

Comprehensive New Massachusetts Privacy Regulations Affect All Businesses with Personal Information of Massachusetts Residents

Stephen E. Meltzer, Esquire, CIPP

[This article was originally drafted and published on March 11, 2009; Updated with amended provisions October 15, 2009]

On Halloween in 2007, the Massachusetts legislature enacted Chapters 93H and 93I of the Massachusetts General Laws to help prevent breaches of security and to protect residents whose information is in the custody of others. In September of 2008, pursuant to Chapter 93H, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) promulgated regulations that define the minimum security standards in connection with the safeguarding the personal information of Massachusetts residents. The "Standards for the Protection of Personal Information of Residents of the Commonwealth" can be found at 201 C.M.R. 17.00, and the new regulations, as amended through August 17, 2009, have a compliance deadline of March 1, 2010. The stated objectives of the regulation are to "insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer."

A majority of states and the federal government have now adopted laws and regulations to protect consumers' personal information. The new Massachusetts regulations, are among the most comprehensive and stringent. The new regulations impose notice requirements for security breaches and carry the potential for significant penalties for noncompliance.

Who is Regulated

Any natural person, corporation, association, partnership or other individual or legal entity that owns or licenses "personal information" about a resident of Massachusetts is subject to the regulations. This would include any person or business that employs Massachusetts residents if its employee records include certain personal information. A business need not have any operations in Massachusetts to be subject to the regulations and the application of the regulations is not limited to any particular industry, and no industry is exempt from the requirements for compliance.

For purposes of the new regulations and Chapter 93H, "personal information" is defined as a Massachusetts resident's first name and last name, or first initial and last name, *combined with* one or more of: "(a) Social Security number, (b) drivers license or state-issued

identification number, or (c) financial account or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account." Lawfully obtained, publically available information is not considered "personal information."

Information Security and Protection

Any business that owns or licenses personal information must "develop, implement, and maintain a comprehensive information security program" to secure and protect records containing personal information that is written in one or more readily accessible parts (a "CWISP").

The program must be "consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated." The program must "contain administrative, technical, and physical safeguards that are appropriate to" (a) the size, scope, and type of the business, (b) the resources available to the business, (c) the amount of stored information, and (d) the need for security and confidentiality of both consumer and employee information. Every program, however, must incorporate at least the following components:

- (a) Designate an employee to maintain the WISP.
- (b) Identify and assess reasonably foreseeable risks (Internal and external).
- (c) Develop security policies for keeping, accessing and transporting records.
- (d) Impose disciplinary measures for violations of the program.
- (e) Prevent access by terminated employees.
- (f) Oversee service providers and contractually ensure compliance.
- (g) Restrict physical access to records.



MELTZER LAW OFFICES

Service. Solutions. Success.

- (h) Monitor security practices to ensure effectiveness and make changes if warranted.
- (i) Review the program at least annually.
- (j) Document responsive actions to breaches.

Computer Security

Any business subject to the new regulations that owns or licenses personal information electronically must include, in its written information security policy, additional technical security procedures to protect its computer system, network, and portable devices including any wireless system. Each computer security policy must have the following elements:

- *Secure User Authentication* – Secure user authentication protocols must be employed. Such procedures must mandate and protect unique user identification and strong passwords, restrict information access to active user accounts, and block access to computer systems after multiple unsuccessful login attempts.
- *Secure Access Control Measures* – Businesses must restrict access to records and files containing personal information to those employees who need such access to perform their jobs and must assign unique identifiers and passwords to each person with computer access.
- *Encryption of Transmitted Information* – All data containing personal information that are transferred over public or wireless networks must be encrypted.
- *Monitoring* – Businesses must monitor all computer systems for unauthorized use or access to personal information.
- *Encryption of Stored Information* – All personal information stored on laptops or portable devices must be encrypted.
- *Firewall Systems and Security Patches* – Any computer system connected to the Internet that contains personal information must be protected with up-to-date firewall protection and operating system patches.
- *Security Software* - Antivirus and malware protection software with up-to-date patches and virus definitions must be installed on any system with personal information.
- *Education and Training* – Businesses must ensure that employees are trained on the proper

use of computer security and the importance of personal information security.

Breach Notification Requirements

Section 3 of Chapter 93H contains specific reporting requirements as well for breaches related to personal information. According to the statute, if the possessor or owner of the information knows, or has reason to know that a breach has occurred, a notification requirement is triggered. The notification must be given if there is a breach of security or if there has been an unauthorized use or acquisition of personal information. Specifically, a possessor (who is not an owner) must notify the owner of the information. The owner must notify the Attorney General, the OCABR and the affected Massachusetts resident.

Data Destruction Requirements

Chapter 93I, which was enacted along with Chapter 93H, contains specific requirements regarding the destruction of data after there is no longer a legitimate need for retention. The Statute requires, with regard to documents in paper form, that they be subject to redaction, burning, pulverizing, and/or shredding such that personal information cannot be read or reconstructed. With respect to personal information stored on electronic media, the media also needs to be destroyed in such a fashion that personal information cannot be read or reconstructed.

Penalties

The Massachusetts Attorney General may bring an action under Chapter 93A, which prohibits unfair and deceptive business practices, for any violation of Chapter 93H and the new regulations. Under Chapter 93A, the business may face temporary or permanent legal injunction, be liable for damages sustained by residents affected by the violation or be subject to statutory civil penalties imposed by the Commonwealth. Violations of the record destruction provisions of Chapter 93I will result in a fine of not more than \$100 per resident affected, up to a maximum penalty of \$50,000 per violation.

What This Means For Your Business

Businesses that own or license personal information should immediately review their existing security policies to ensure compliance with the new regulations or, if they do not have such policies, they need to act quickly to develop a comprehensive program that incorporates all of the new requirements before the effective date.



MELTZER LAW OFFICES
Service. Solutions. Success.