R McHale LLC

Data Security & Identity Theft:

NEW PRIVACY REGULATIONS THAT AFFECT YOUR BUSINESS

Robert McHale, Esq.

Effective March 1, 2010, all businesses that own or license personal information of Massachusetts residents are required to comply with comprehensive information security regulations adopted by the Massachusetts Office of Consumer Affairs and Business Regulation. This article discusses what the law requires and what your business needs to do today to comply.

Table of Contents

PRACTICE POINT

The regulations apply to any business, WHETHER OR NOT OPERATING IN MASSACHUSETTS, if such business owns, licenses, receives, maintains, processes or otherwise has access to personal information of Massachusetts residents. Potentially every business may find itself subject to the regulatory requirements.

Introduction

Effective March 1, 2010, all businesses that own or license personal information of Massachusetts residents are required to comply with comprehensive information security regulations adopted by the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR).[1]

The regulations – entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth" – are by far the most strident and far-reaching of any information security regulations of any state to date.

The regulations are designed to insure the security and confidentiality of personal information of Massachusetts residents; to protect against anticipated threats to the security or integrity of such information; and to protect against the unauthorized access to or use of such information in a manner that may result in substantial harm or inconvenience to any consumer.[2]

Because the regulations affect virtually every entity conducting business in Massachusetts, it is imperative that companies implement proper information security programs to comply with the regulations.

Background

In 2007, Massachusetts joined 38 others states and enacted data breach notification laws. Chapter 93H requires entities that own or license personal information of Massachusetts residents to publicly report the unauthorized acquisition or use of compromised data.[3]

Significantly more aggressive than similar legislation from other states, Chapter 93H also mandates the adoption of detailed information security regulations for businesses in order to reduce the number of security breaches and thereby the need for data breach notifications.

The resulting regulations (201 CMR § 17.00 et seq.) establish minimum standards by which a company is required to safeguard the integrity of personal information it handles.

PRACTICE POINT

A company's information security program must be in writing.

PRACTICE POINT

Terminated employees' physical and electronic access to records containing personal information should be immediately blocked, including deactivating their passwords and usernames.

PRACTICE POINT

Companies must require that their third-party service providers contractually agree that they have appropriate security measures for personal information.

Requirements

The regulations impose detailed administrative and technical obligations on any person that owns, licenses, stores or maintains personal information of Massachusetts residents.

Administrative Requirements[4]

The regulations require businesses to comply with the following administrative obligations:

- *Program Implementation and Oversight.* Companies must designate one or more employees to maintain and enforce a comprehensive information security program.
- *Security Policies.* Companies must create policies governing whether and how employees keep, access and transport records containing personal information outside of business premises. Companies must also impose disciplinary measures for violations of its comprehensive information security program rules.
- *Limited Access.* Companies must impose reasonable restrictions upon physical access to records containing personal information.
- *Monitoring.* Companies must regularly monitor the information security program to ensure its proper operation and effectiveness.
- *Security Breaches.* Companies must document responsive actions taken in connection with any incident involving a security breach.
- *Service Providers.* Companies must take reasonable steps to ensure that third-party service providers with access to personal information have the capacity to protect such information consistent with the Massachusetts regulations and applicable federal regulations.

PRACTICE POINT

Companies will probably need to hire an IT professional to verify that their computer systems comply with the encryption requirements. At a minimum, the encryption process must transform the personal information in such a way that it cannot be understood without the use of a confidential key.

Technical Requirements[5]

The regulations also impose significant technical requirements for any computers, systems, or networks involved in the maintenance or transmission of personal information.

Specifically, the regulations require companies to establish and maintain a comprehensive information security program incorporating, at a minimum, and to the extent technically feasible, the following elements:

- *User Authentication Protocols.* Companies must implement secure user authentication protocols including:
  - i) control of individual account identifiers to limit access
  - ii) secure measures for selecting, storing and accessing passwords
  - iii) control of data security passwords to ensure that passwords are kept in a location and/or format that does not compromise the data they protect
  - iv) restricting access to active users only; and
  - v) blocking access to user identification after multiple unsuccessful attempts to gain access
- *Access Controls.* Companies must implement secure access control measures that:
  - i) restrict access to records and files containing personal information on a "need-to-know" basis
  - ii) assign unique identifications plus passwords to each person with computer access
- *Encryption.* Companies must encrypt all personal information when stored on laptops or other portable devices, or in transit across public networks or by wireless connection.
- *Monitoring.* Companies must monitor their systems to detect unauthorized access to or use of personal information.
- *Firewall Protection.* Companies must use reasonably up-to-date firewall protection and system security agent software (including malware protection) for files containing personal information on a system connected to the Internet.
- *Antivirus Protection.* Companies must also have reasonably up-to-date antivirus software and security patches.
- *Employee Training.* Companies must educate and train their employees on the proper use of the computer security system and the importance of personal information security.

Who Is Subject To The Regulations?

The regulations apply to all persons that own, license, store or maintain personal information about a Massachusetts resident.[6] The regulations specifically apply to:

- Natural persons
- Corporations (or other business entities)
- Associations
- Partnerships

PRACTICE POINT

"Personal information" does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

What Is "Personal Information"?

"Personal Information" is defined to include a Massachusetts resident's first and last name (or first initial and last name) combined with any one or more of the following elements relating to such resident:

- Social Security number
- Driver's license number or state-issued identification card
- Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password[7]

What Type Of "Records" Are Included?

The regulations define "records" to include any material upon which written, drawn, spoken, visual or electromagnetic information or images are recorded, regardless of physical form or characteristics.[8]

The following records therefore are subject to the regulations:

- Personnel records
- Payroll records
- Electronic records
- Credit card information
- Customer records

PRACTICE POINT

There is no one-size-fits-all model to measure compliance. The regulations establish minimum requirements. Your company should implement further measures specific to it.

How Is Compliance Judged?

The regulations attempt to strike a balance between the legitimate needs of businesses seeking to avoid costly and burdensome administrative and technical requirements, and the privacy and security interests of Massachusetts residents.

The regulations have therefore adopted a "reasonableness" standard by which to measure compliance. For example, persons must use "a reasonably secure method of assigning and selecting passwords,"[9] adopt "reasonable restrictions upon physical access to records containing personal information,"[10] and employ "reasonably up-to-date firewall protection"[11] and "reasonably up-to-date versions of system security agent software."[12]

Further, compliance with the regulations shall be evaluated taking into account the entity's size, scope and amount of resources, together with the amount of stored data and the need for security and confidentiality of both consumer and employee information.[13]

Conclusion

Given the fast-approaching March 1, 2010 deadline, compliance with the data security regulations may prove daunting for many businesses.

It is critical that companies begin implementing conforming information security programs as soon as practicable.

Any company handling personal information of Massachusetts residents should act now to ensure timely and proper regulatory compliance.

If you would like additional information, please contact:

Robert McHale, Esq.
R | McHale LLC
9 West Broadway, Suite 422
Boston, Massachusetts 02127
Tel: (617) 306-2183
Fax: (617) 848-9483
E-mail us now

Endnotes

1 201 Code of Mass Regulations § 17.00 et seq.

2 201 Code of Mass Regulations § 17.01(1).

3 Mass. General Laws, Chapter 93H.

4 201 Code of Mass Regulations § 17.03.

5 201 Code of Mass Regulations § 17.04.

6 201 Code of Mass Regulations § 17.01(2).

7 201 Code of Mass Regulations § 17.02.

8 201 Code of Mass Regulations § 17.02.

9 201 Code of Mass Regulations § 17.04(1)(b).

10 201 Code of Mass Regulations § 17.03(g).

11 201 Code of Mass Regulations § 17.04(6).

12 201 Code of Mass Regulations § 17.04(7),

13 201 Code of Mass Regulations § 17.03(1).

About R | McHale LLC

R | McHale LLC is a premier, Boston-based law firm offering comprehensive legal services in the following practice areas: Corporate Law, Litigation, and Business Immigration.

We are privileged to represent individuals, emerging ventures, small- and mid-sized companies, and prominent national and multinational corporations involved in sophisticated business transactions and complex legal disputes.

Our mission is simple: to provide exceptional and unparalleled client service.

Knowing that our clients' success is our success, we deliver customized solutions for the full spectrum of our clients' legal needs, providing top-tiered professional counsel at tremendous value.

R | McHale LLC provides expert advice that makes both legal and business sense.

Stay Connected

Connect to Robert McHale via Linkedin

Subscribe to R | McHale LLC Publications

Contact Information

Robert McHale, Esq.
R | McHale LLC
9 West Broadway, Suite 422
Boston, Massachusetts 02127
Tel: (617) 306-2183
Fax: (617) 848-9483
E-mail us now