

TOUGH NEW STANDARDS FOR PERSONAL INFORMATION PROTECTION

Massachusetts has taken the lead in requiring businesses to develop and implement a comprehensive security program intended to protect from unauthorized disclosure the person information of the state's residents.

Every person or business that owns, licenses, stores or maintains personal information about a resident of Massachusetts will now be required to develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information.

What Must Be Included In The Security Program:

Included in the regulation are these minimum elements:

- Identification and assessment of risks.
- Evaluation and improvement of the effectiveness of safeguards.
- Development of security policies for employees.
- Taking reasonable steps to verify third-party service providers have the capacity to protect information.
- Obtaining from third-party service providers a written certificate that they are in compliance.
- Limits on the amount of personal information collected, the time such information is retained, and the access to such information.

While the first part of the regulation requires the implementation of a comprehensive security program, the second imposes certain security system requirements for computer and wireless networks which would include the use of secure user authorization protocols, secure access control measures, encryption of stores and transmitted data, and Internet firewall protections. These requirements are quite tough and will most likely require businesses to revise or create new information security programs and policies to comply with these regulations by the first effective date of May 1, 2009.

To Whom They Apply:

The new regulations are intended to apply to "all persons that own, license, store or maintain personal information about a resident" of Massachusetts. Personal information is defined as first and last name, or first initial and last name, in conjunction with any one or more of the following:

- Social security number
- Driver's license number (or state-issued id card number)
- Financial account number of credit or debit card number

Penalties for Non-Compliance:

Violators may be subject to a \$5,000 civil penalty for each violation. Worst-case scenarios include outcomes that are mind boggling in scope. For example, if a business maintains 10,000 records that contain personal information of Massachusetts residents and the business is not in compliance, it may be possible that the business could be assessed up to \$50 million in civil penalties.

Key Dates & Requirements

201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth of Massachusetts

• May 1, 2009

The general compliance deadline. This date is consistent with a new FTC Red Flag Rule which requires financial institutions and creditors to develop and implement written identity theft prevention programs. Businesses addressing the new FTC requirements can now address the state regulations during the same time frame. This is also the deadline for ensuring that third-party service providers are capable of protecting personal information and contractually binding them to do so; and, the deadline for ensuring encryption of laptops.

• Jan 1, 2010

The deadline for requiring written certification from third-party providers. This is also the deadline for ensuring encryption of portable devices other than laptops such as memory sticks, DVDs and PDAs.

Additional Resources: [Massachusetts Office of Consumer Affairs & Business Regulation](#)

Mazonson LLC

Managing risk. Empowering growth.