Consumer Affairs Agencies

Division of Banks
Division of Insurance
Division of Professional Licensure
Department of Telecommunications and Cable
Division of Standards
State Racing Commission

Daniel C. Crane
Undersecretary

10 Park Plaza
Suite 5170
Boston, MA 02116

Hotline:
617-973-3787
888-283-3757

www.mass.gov/consumer

FREQUENTLY ASKED QS

Chapter 82 of the Acts of 2007
"An Act Relative to Security Freezes and Notification of Data Breaches"
Massachusetts Security Breaches Law

What is a security breach?
A security breach occurs when there is an unauthorized acquisition of unencrypted data that can be used to compromise the security, confidentiality, or integrity of personal information and creates a substantial risk of identity theft or fraud. Acquisition or use of encrypted data along with the encryption key would also be considered a security breach.

What constitutes a reportable event?
If a person who is holding information knows of a security breach, or that personal information was acquired by an unauthorized person or used for an unauthorized purpose, then a reportable event has occurred.

When a security breach has occurred, who is a company required to notify?
If a reportable event has occurred, the company is required to notify the Office of Consumer Affairs and Business Regulation (OCABR) and the Attorney General as well as the affected party. The law also requires that when a company reports a breach that it also provide details of the steps that have been taken to prevent a breach from happening again.

How will this new law affect businesses in Massachusetts?
These regulations apply to all companies conducting business in Massachusetts, large and small, who compile or maintain records that include personal information. Companies will need to establish and maintain a security program for the protection of personal information. The regulations call on businesses to encrypt data sent over the Internet or saved on laptops or flash drives; encrypt wirelessly transmitted data; and to utilize up-to-date firewall protection that creates an electronic gatekeeper between the data and the outside world and only permits authorized users to access or transmit data, according to preset rules.

What changes will companies need to make?
Many companies may already have most, if not all, of the required measures in place to protect personal information. Some companies may simply need to activate security features in hardware and software that are already in place on their computer systems and networks while other companies that currently conduct no protective maintenance on its data records may incur an incremental cost to enhance its technical oversight.

How will we know which companies are following the rules and which ones are not?
As with most laws, we will discover who is not playing by the rules when a breach occurs and it is investigated. No company is exempt from these requirements and the Attorney General has the enforcement role under the statute.

If a company complies with federal Graham-Leach-Bliley or HIPAA requirements, do they have to comply with these new regulations as well?

Yes. These regulations are not pre-empted because both GLB and HIPAA allow state laws to provide for a higher standard of protection.

How can a company determine that the vendors they work with are complying with the regulations?

The vendor will need to sign a document that says that it has a written, comprehensive information security program that is in compliance with the provisions of the regulations.

When do the regulations become effective?

The regulations become effective on January 1, 2009. Prior to the effective date, a company must complete internal and external security risk assessments and provide training to its employees.

Has the state provided guidelines for a security program?

While each company will need to adopt a plan that complies with the new regulations and considers its specific business operations, the Office of Consumer Affairs and Business Regulation will provide a model plan as a guideline by October 1st.