Massachusetts Adopts Strict Data Security Regulations

As security breaches at major businesses continue to generate headlines, the Massachusetts Office of Consumer Affairs and Business Regulation has issued groundbreaking new regulations which impose significant requirements on companies that have personal information about Massachusetts residents.

Effective January 1, 2009, the regulations require companies to develop a comprehensive security program to safeguard any electronic or paper record that contains such information. In addition, companies that electronically store or transmit such information must ensure that their computer systems meet a number of specific technical requirements and must provide security training to their employees.

These regulations are the latest in an emerging trend of increased state regulation in the information security area. They are the most far-reaching and technically specific of virtually any existing state data security laws, and their technical requirements exceed federal data security regulations and guidance. With the effective date only a few months away, companies need to immediately assess their security program and take prompt action to ensure compliance with the new rules. This alert highlights several features of the regulations.

Who is Subject To The Regulations?

Issued on September 19, 2008 pursuant to the security breach notification law that Massachusetts enacted last year (Mass. Gen. L. ch. 93H), the "Standards for the Protection of Personal Information of Residents of the Commonwealth" (201 C.M.R. 17.00) apply to all persons (including corporations and other entities) that own, license, store, or maintain personal information about a Massachusetts resident. The term "personal information" is defined, as it is in most states' breach notification laws, to mean a person's name *in combination with* certain sensitive items, such as a Social Security number, driver's license number, financial account number, or debit or credit card number.

This definition of "personal information" reaches a wide variety of records commonly kept by organizations in many different industries, such as records containing employee information, customer information, investor information, patient information, or student information. An important limitation, however, is that the definition includes only those records which contain *both* a resident's name *and* certain sensitive personal information. As a result, some consumer records, such as credit card numbers standing alone, are not subject to the regulations.

Information Security Program

The regulations require companies to implement and maintain a comprehensive, written program to protect the security and confidentiality of personal information. This program must be "reasonably consistent with industry standards," taking into account the company's size and scope, the amount of resources available to the company, and the amount of personal information the company stores. A key component is for companies to engage in an ongoing process of assessing risks to personal information and addressing those risks through the use of administrative, physical, and technical safeguards. This requirement is similar to the requirements that federal regulations impose on financial companies (e.g., Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., enforced under FTC "Safeguards Rule," 16 C.F.R. § 314).

In addition, the program must include a variety of specific safeguards, many of which are not found in any other state or federal data security laws. Some of the more noteworthy examples include:

- *Data Inventory:* Companies must conduct a data inventory to identify where they are storing personal information, both in electronic and paper form.

- *Data Retention:* Companies must limit the amount of personal information that they retain and the length of time they retain it to only that which is reasonably necessary.
- *Need-to-Know Access:* Companies must limit access to personal information on a need-to-know basis and must terminate immediately the access of employees who leave the company.
- *Service Providers:* Companies must take reasonable steps to verify that outside service providers, if given access to personal information, have the capacity to protect it. Before allowing a service provider to access personal information, companies must obtain a written certification that the service provider has an information security program that complies with the Massachusetts regulations.
- *Security Policies:* Companies must develop security policies for their employees, particularly with respect to off-site use of personal information. They also must impose disciplinary measures for security violations.
- *Security Incidents:* Companies must document responsive actions taken in connection with any incident involving a security breach, including any changes in their business practices.

Computer System Security Requirements

For companies that electronically store or transmit personal information, the regulations also impose a host of technical security requirements that the company's computer systems must meet. These requirements include:

- *Encryption:* Companies must encrypt personal information when it is stored on laptops or other portable devices, when it is transmitted over wireless systems, and (to the extent feasible) when it travels across public networks.
- *Access Controls:* Companies must implement secure user authentication protocols and secure access control measures, including unique user identification and other detailed requirements.
- *Monitoring:* Companies must reasonably monitor their systems for unauthorized access to or use of personal information.
- *Antivirus and Patching:* Companies must have "reasonably up-to-date" antivirus software and security patches.
- *Segmentation:* Companies also must have "reasonably up-to-date" firewall protection.
- *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.

Enforcement

The statute under which the regulations were issued (Mass. Gen. L. ch. 93H) authorizes the Massachusetts Attorney General to remedy violations by bringing an action under the state's "Little FTC Act" (Mass. Gen. L. ch. 93A), which prohibits unfair or deceptive business practices and, in some instances, authorizes civil penalties.

Compliance Challenge

Complying with these new regulations will present a challenge for companies. The design and implementation of a comprehensive information security program, especially one that must meet specific technical requirements, can require considerable time and resources, as well as careful planning and oversight. Companies that handle the personal information of Massachusetts residents should act quickly to ensure compliance with the new regulations by the deadline of January 1, 2009.

If you would like to learn more about the issues raised by this update, please contact any of the following members of our Privacy Group: partners Lisa M. Ropple (617-951-7554) and David McIntosh (617-951-7875) and associates Kevin Jones (617-951-7345) and Christine Santariga (617-951-7185).