Massachusetts' Strict Data Security Regulations, Effective March 1, 2010, Pose Compliance Challenge for Many Organizations, Including Colleges, Universities, and Health Care Providers

As security breaches at major businesses continue to generate headlines, colleges, universities, health care providers, and any other organizations that own or license personal information of Massachusetts residents will soon be required to comply with Massachusetts' groundbreaking information security regulations. These regulations require organizations to develop a comprehensive written information security program to safeguard any electronic or paper record that contains such information. In addition, organizations that electronically store or transmit such information must ensure that their computer systems meet a number of specific technical requirements, including encryption of certain data, and must provide security training to their employees. The rule applies to a broad array of organizations, and institutions located outside of Massachusetts may be unaware that the regulations apply to their handling of information relating to Massachusetts residents.

Despite several delays in the deadline for compliance, the regulations will now take effect on March 1, 2010. These regulations are the latest in an emerging trend of increased state regulation in the information security area. They are arguably the most far-reaching and technically specific state data security laws enacted to date. Their technical requirements exceed federal data security regulations and guidance. With the effective date less than a month away, any organization that stores, handles, or accesses personal information of Massachusetts residents needs to assess its security program and take prompt action to ensure compliance with the new rules. This alert highlights several features of the regulations. The scope and breadth of the regulations have generated public controversy and, in response, caused several revisions since the regulations were first issued in September 2008. Our discussion of this process and the resulting revisions can be found in previous alerts (9/29/08 Alert, 11/20/08 Alert, 2/13/09 Alert, 10/2/09 Alert and 11/13/09 Alert).

Who is Subject To The Regulations?

Issued pursuant to the Massachusetts security breach notification law (Mass. Gen. L. ch. 93H), the regulations apply to all persons (including corporations and other entities) that own or license personal information about a Massachusetts resident. The regulations define "personal information" as a Massachusetts resident's name in combination with certain information about the resident, such as his or her 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 student information, employee information, customer information, investor information, and patient information.

Information Security Program

The regulations require organizations to implement and maintain a comprehensive, written program to protect the security and confidentiality of personal information. This program must contain administrative, technical, and physical safeguards that take into account the organization's size, scope, and business; amount of resources available to the organization; amount of stored data; and the need for security and confidentiality of consumer and employee information. The law specifies that both an organization's implementation of its program, as well as Massachusetts' evaluation of such program, should follow a risk-based approach. Finally, the safeguards contained in the information security program must be consistent with other applicable state and federal requirements.

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:

- *Identification and Evaluation of Risks:* Organizations must identify and assess reasonably foreseeable risks to the security, confidentiality, and integrity of any records that contain personal information and evaluate and improve the effectiveness of current safeguards, including ongoing employee training and employee compliance with policies and procedures.
- *Physical Access Restrictions:* Organizations must develop reasonable restrictions for physical access to records that contain personal information as well as for storage of records and data in locked facilities or containers. They must also immediately terminate the access of employees who leave the organization.
- *Monitoring:* Organizations must regularly monitor and review the scope of the security measures to ensure that the information security program is operating to prevent unauthorized access to, or use of, personal information.
- *Security Policies:* Organizations 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:* Organizations must document responsive actions taken in connection with any incident involving a security breach, including any changes in their business practices.
- *Service Provider Requirements:* Service providers are defined as "any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation . . ." Organizations must select and retain third party service providers that are capable of maintaining security measures consistent with the state regulations and any applicable federal requirements. Organizations that retain service providers on or after March 1, 2010 must require such providers by contract to implement and maintain appropriate security measures for personal information. Organizations have until March 1, 2012 to amend contracts executed before March 1, 2010 to include personal information security provisions.

Computer System Security Requirements

For organizations that electronically store or transmit personal information, the regulations also impose a host of technical security requirements that the organization's computer systems, at a minimum, and to the "extent technically feasible," must meet. These requirements include:

- *Encryption:* Organizations must encrypt personal information when it is stored on laptops or other portable devices, when it is transmitted over wireless systems, and when it travels across public networks.
- *Access Controls:* Organizations must implement secure user authentication protocols and secure access control measures, including unique user identification and other detailed requirements.

- *Monitoring:* Organizations must reasonably monitor their systems for unauthorized access to, or use of, personal information.
- *Antivirus and Patching:* Organizations must have "reasonably up-to-date" antivirus software and security patches.
- *Segmentation:* Organizations also must have "reasonably up-to-date" firewall protection.
- *Employee Training:* Organizations 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 May be Challenging

Complying with the Massachusetts regulations presents a challenge for many organizations, especially those that own or maintain other types of information, such as health care providers that maintain protected health information. Colleges, universities, health care providers, and other types of organizations are also subject to other laws, both federal and state, that relate to data privacy and security. For these types of organizations, an analysis of existing policies and procedures will need to be undertaken to ensure compliance with all applicable laws and regulations. In addition, organizations must assess their service provider relationships and ensure that contracts containing appropriate information security provisions are in place in accordance with the timeline set forth in the regulations. The design and implementation of a comprehensive information security program can require considerable time and resources, as well as careful planning and oversight. Organizations that handle the personal information of Massachusetts residents should act quickly to ensure compliance with the relevant requirements by March 1, 2010.

If you would like to learn more about the issues raised by this update, please contact your usual Ropes & Gray attorney.