Massachusetts Extends Compliance Deadlines for Data Security Regulations Again

On Thursday, February 12, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) extended the deadline for compliance with Massachusetts' groundbreaking information security regulations for the second time. Companies that have personal information about Massachusetts residents now have until January 1, 2010 to implement a comprehensive information security program and specific computer system security requirements. The latest amendment also revises the requirement related to service provider contractual obligations and eliminates the requirement to obtain a certification from service providers that handle personal information.

The Regulations

As explained in Ropes & Gray's previous alert, the new "Standards for the Protection of Personal Information of Residents of the Commonwealth" (201 C.M.R. 17.00) require all entities that own, license, store, or maintain personal information about Massachusetts residents to develop a comprehensive information security program. In addition, entities 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.

The regulations define "personal information" to mean a Massachusetts resident'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.

Initial Revisions

When the regulations were first issued on September 19, 2008, they carried an effective date of January 1, 2009, which would have given companies only a few months to achieve compliance with all of the requirements.

In response to public outcry about the aggressive deadline and in light of broader economic conditions, on November 14, 2008, the OCABR extended the deadline for complying with the regulations generally until May 1, 2009. The agency also established a separate deadline of January 1, 2010 for what it perceived to be the most burdensome requirements: (i) obtaining a written certification from any service provider that would have access to personal information, attesting that the service provider complies with the Massachusetts regulations, and (ii) encrypting personal information stored on portable devices other than laptops (such as handheld PDAs, memory sticks, and DVDs).

Latest Revisions

In its latest revision on February 12, 2009, the OCABR responded to escalating concerns from business leaders and companies who argued that that the deadlines were still too aggressive and the service provider requirements were still too burdensome.

Extended Deadline: The new revision extends the compliance deadline for all of the requirements to January 1, 2010, thereby dispensing with the phased compliance structure created by the earlier revision.

Service Provider Requirements: The new revision clarifies the service provider requirements and dispenses with the certification requirement. This change alleviates confusion and possible administrative burdens for some companies that may have resulted from having separate contractual and certification requirements with different deadlines. Under the current regulations, companies now must:

- Take all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect it in the manner provided for in the regulations; and
- Take all reasonable steps to ensure that such third-party service provider applies protective security measures at least as stringent as those required to be applied to personal information under the regulations.

Compliance May Still Be Challenging

Despite the extended deadline and additional flexibility, complying with the new Massachusetts regulations will continue to present a challenge for many companies. The design and implementation of a comprehensive information security program can require considerable time and resources, as well as careful planning and oversight. Companies that handle the personal information of Massachusetts residents should continue to develop a programmatic solution to ensure compliance with the relevant requirements by January 1, 2010.

If you would like to learn more about the issues raised by this update, please contact your usual Ropes & Gray attorney, or any of the following members of our Data Privacy Group: Lisa M. Ropple, David M. McIntosh, Kevin V. Jones, or Christine M. Santariga.