Massachusetts Extends Compliance Deadlines for New Data Security Regulations

On November 14, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) extended the deadlines for companies to comply with new, groundbreaking Massachusetts regulations which impose significant requirements on companies that have personal information about Massachusetts residents. Companies now have until May 1, 2009 to comply with the regulations generally and until January 1, 2010 to comply with specific requirements relating to the certification of outside service providers and the encryption of certain portable devices.

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 Social Security, driver's license, financial account, debit or credit card numbers.

The New Deadlines

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. Business groups warned that this aggressive deadline would be overly burdensome or even impossible to meet, given the unprecedented scope and technical specificity of the regulations. In response to this public outcry and in light of current economic conditions, the OCABR recently announced that it has extended the compliance deadlines as follows:

For Compliance Generally. The agency extended the general deadline for complying with regulations until May 1, 2009. As the agency noted, this new deadline coincides with the deadline for complying with the Federal Trade Commission's new "Red Flag Rule," 16 C.F.R. Part 681, which requires financial institutions and creditors to develop and implement written programs to detect and prevent identity theft.

For Certification of Service Providers. The agency established a separate deadline of January 1, 2010 for the requirement that companies, before permitting outside service providers to access personal information, obtain written certification that the service provider complies with the Massachusetts regulations. All of the other requirements relating to outside service providers, however, will be effective on May 1, 2009, including the requirements that companies take reasonable steps to verify that service providers with access to personal information have the capacity to protect it and that they contractually agree to maintain safeguards.

For Encryption of Certain Portable Devices. The agency also established a separate deadline of January 1, 2010 for the requirement that companies encrypt personal information stored on portable devices other than laptops (such as handheld PDAs, memory sticks, and DVDs). Companies still must encrypt personal information stored on laptops by the general compliance deadline of May 1, 2009.

Compliance May Still Be Challenging

Even with the extended deadlines, complying with the new Massachusetts regulations will 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 act quickly to ensure compliance with the relevant requirements by May 1, 2009.

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, Christine M. Santariga.