CLIENT ALERT

Massachusetts Sets the New Standard, But Delays Implementation

Dec.04.2008

The Commonwealth of Massachusetts recently issued final regulations, implementing its security breach notification statute, that mandate privacy and security standards for all organizations that own, license, store or maintain personal information about Massachusetts residents. Virtually every company that has employees or customers in Massachusetts will be affected by these regulations. These state regulations are the first of their kind in the US and mirror some of the requirements of the more robust European data protection laws or the regulations implementing the Gramm-Leach-Bliley Act, which pertain to banking and financial institutions. However, the Massachusetts regulations may provide a glimpse into what's next for state legislatures around the country.

The original deadline for compliance was January 1, 2009; however, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) announced on November 14th that it would extend the deadline to May 1, 2009. The OCABR said that "in light of intervening economic circumstances," it delayed the deadline to "provide flexibility to businesses that may be experiencing financial challenges brought on by national and international economic conditions." OCABR said the deadline for ensuring that third-party service providers are capable of protecting personal information and contractually binding them to do so will be extended from January 1, 2009 to May 1, 2009, and the deadline for requiring written certification from third-party providers will be further extended to January 1, 2010. The agency said the tiered deadlines for requiring certification will ensure proper consumer protection and facilitate implementation without overburdening small businesses during harsh economic times. The deadline for ensuring encryption of laptops will be extended from January 1, 2009 to May 1, 2009, and the deadline for ensuring encryption of other portable devices will be suspended until January 1, 2010.

The new regulations build on the Massachusetts security breach notification law, which mandated the development of the regulations to "safeguard the personal information of residents of the commonwealth." The objectives of the regulations, as set forth in the breach law, are to: "insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to a consumer." Personal information is defined for these purposes as "a resident's first name and last name or first initial and last name in combination with any one of more of the following: social security number; driver's license number or state-issued identification card number; or financial account number or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account."

Most importantly, the new regulations add teeth to a key requirement of many security breach notification laws - that organizations ensure "reasonable and adequate security" - by delineating specific technical security measures that any covered organization must adopt, including:

- secure user authentication protocols
- secure access control measures

- encryption of all transmitted personal information that travels across public networks and wirelessly (to the extent technically feasible)
- reasonable monitoring of systems for unauthorized use or access
- encryption of all personal information stored on laptops or other portable devices (nothing about feasibility on this one)
- up-to-date firewall protections and OS patches
- reasonably updated versions of system security agent software which must include malware, patches and virus definitions
- education and training of employees on the proper use of the computer security system and the importance of personal information security

The Massachusetts regulation also mandates a comprehensive, written security program applicable to all personal information. The written program must include:

- designation of a person responsible for the program
- an assessment of risks and safeguards to limit those risks
- polices that address employee handling of personal information outside of business premises
- disciplinary measures for violations of the program
- measures to prevent access to personal information by terminated employees
- verification that third party providers who handle personal information have adequate safeguards and a written certification that the vendor has met the standards set forth in the Massachusetts regulation
- limitations on the collection, retention of, and access to personal information
- a description of the location of personal information within the organization
- restrictions on physical access to personal information
- a plan to monitor and upgrade the program regularly
- at least annual reviews of the scope of the program
- a process to document responses to any security breach

Those doing business in Europe, or in the health care or financial industries, should be well on their way to compliance with the new regulations. Others may need to take a closer look at their privacy and security standards to ensure that they are ready for the new Massachusetts regulations when they take effect on May 1, 2009 and January 1, 2010.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kris D. Meade
Partner – Washington, D.C.
Phone: +1 202.624.2854
Email: kmeade@crowell.com