Massachusetts Proposes Amendments and a Further Extension of the Compliance Deadlines for Data Security Regulation

On August 17, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) proposed extending the deadline for compliance with Massachusetts' groundbreaking information security regulation for the third time. If the proposed regulation is approved, companies that have personal information about Massachusetts residents will have until March 1, 2010 to implement a comprehensive written information security program and to ensure that their computer systems meet a number of specific computer system security requirements. The latest revision also modifies the regulation to make it more flexible. In its press release accompanying the revision, the OCABR said that the changes are intended to balance consumer protections with business concerns. A hearing is scheduled for September 22, 2009 to provide an opportunity to comment on the regulation. The comment period ends on September 25, 2009.

The Regulation

Issued pursuant to the Massachusetts security breach notification law (Mass. Gen. L. ch. 93H), the proposed "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 or license personal information about a Massachusetts resident, *i.e.*, any company that "receives, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment." The regulation defines "personal information" as a Massachusetts resident's name in combination with certain information about the resident, such as, among other things, his or her Social Security number, driver's license number, financial account number, or debit or credit card number.

Initial Revisions

When the regulation was first issued on September 19, 2008, it 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, the OCABR extended the compliance date twice, first to May 1, 2009 (with certain requirements extended until January 1, 2010) and then until January 1, 2010 for all requirements.

In previous alerts, Ropes & Gray described the initial release (click here) and the first two revisions of the regulation (click here and here).

Latest Revisions

In its latest revision on August 17, 2009, the OCABR responded to continuing concerns from business leaders and companies, especially small companies, who argued that the deadlines were still too aggressive and that many requirements were still too burdensome. The new revisions contain several modifications that are consistent with an overall risk-based approach.

Purpose: The objective of the proposed regulation is 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 any consumer." The last phrase is potentially broader than prior versions, which focused on unauthorized access or use of information that "creates a substantial risk of identity theft or fraud" against residents.

Although the new purpose statement specifically references "customers" and "consumers," the proposed regulation, taken as a whole, continues to apply to both customer or consumer information and employee information.

Information Security Program: The current revision makes clear that a company's written information security program should take into account the size and nature of the business, amount of resources available to the company, amount of stored data, and the need for security and confidentiality of consumer and employee information. The revised language clarifies that both a company's implementation of its program, as well as the Commonwealth's evaluation of such program, should follow a risk-based approach. The proposed regulation also clarifies that the program must be consistent with other applicable state and federal regulations.

Service Providers: A "service provider" is defined in the proposed regulation as "any person that receives, 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; provided, however, that 'service provider' shall not include the U.S. Postal Service."

The current revision clarifies and softens companies' obligations with respect to such service providers. The prior version required companies to verify that any third-party service provider with access to personal information possessed the capacity to protect it in the manner provided for in the regulation and to ensure that the service provider applied protective security measures at least as stringent as required under the regulation. The proposed regulation, however, requires companies to "select and retain third party service providers that are capable of maintaining security measures consistent with the regulations and any applicable federal requirements."

The proposed regulation also specifies that companies retaining service providers on or after March 1, 2010 must require such service providers by contract to implement and maintain appropriate security measures for personal information. Although the regulation is somewhat confusing on this point, the OCABR has said that service provider contracts entered into before March 1, 2010 will be deemed in compliance with the regulations for a two-year grace period (until March 1, 2012), even if such contracts do not contain the requisite provisions related to security measures. This responds to a key area of concern among companies regarding the potential costs and resource constraints of amending all existing service provider contracts as of the effective date of the regulation.

Data Identification, Minimization, and other Eliminated Program Requirements: The current revision eliminates previous requirements for companies to identify all documents and media where personal information is located, which some companies interpreted as an inventory process. It also eliminates a requirement to limit the amount of personal information collected and retained to that which is reasonably necessary to accomplish the original legitimate purpose. Other specific requirements are eliminated in favor of more general language. For example, the requirement to prevent terminated employees from accessing records containing personal information no longer requires a company to "immediately" terminate such access. The OCABR states in its FAQs that these eliminated requirements "will be used as a form of guidance only."

Computer Security Requirements and Encryption: The current revision specifies that the computer system security requirements apply where they are "technically feasible," which the OCABR defines in its FAQs to mean that "if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used." This change applies the risk-based approach of the regulation to the unique challenges presented by businesses of various sizes.

The revision also makes the "encryption" requirement technology neutral by defining it as "the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key." This change is meant to address the evolution of encryption technology, so that the regulation will not impede the adoption of any new technologies.

Compliance May Still Be Challenging

The current revision represents proposed regulations that, once approved, would become effective on March 1, 2010. Despite the extended deadline and additional flexibility, complying with the new Massachusetts regulation 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 March 1, 2010.

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