Massachusetts Consumer Protection Authority Finalizes Data Security Regulations

The Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) recently announced that it had filed the "final" version of the "Standards for the Protection of Personal Information of Residents of the Commonwealth" (201 C.M.R. 17.00) with the Secretary of State's office. After just over a year of amendments to the original regulations, first issued in September 2008, this filing is the final step before the regulations take effect March 1, 2010. The final regulations include some clarifications, but are substantially similar to the most recent set of amendments released in August 2009.

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.

Given the broad scope of the regulations, the specificity of the requirements, and general economic conditions, the regulations have generated a substantial amount of public outcry. In response, the OCABR has amended the regulations several times since their initial release. Ropes & Gray described the initial release and the first three revisions of the regulations, in greater depth in previous alerts (9/29/2008 Alert, 11/20/08 Alert, 2/13/09 Alert, and 10/2/09 Alert).

Latest Revisions

The final regulations are substantially similar to the prior version with some wording changes, many of which were in response to requests from companies and business leaders for clarification.

Definition of Owns or Licenses. A company owns or licenses personal information if it "receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment." The final regulations make clear for the first time that a company that "stores" the personal information of a Massachusetts resident is subject to the regulations' requirements, even if the company does not otherwise process or access such information.

Definition of Service Providers. A service provider is 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." The final regulations eliminate a previous carve-out that had stated, "'service provider' shall not include the U.S. Postal Service." It is not clear that the OCABR intends this change to mean that a company using the U.S. Postal Service to transmit personal information must contractually require the U.S. Postal Service to implement and maintain appropriate security measures for such personal information, as it must do with other service providers. But the OCABR has stated that a company must assess the risks of using a common carrier, including the U.S. Postal Service, to transmit personal information and take steps to protect that personal information.

Amending Existing Contracts with Service Providers. The final regulations clarify prior language related to a grace period for amending existing contracts with service providers so that such contracts require the service providers to implement and maintain appropriate security measures for personal information. The regulations now make clear that a company has until March 1, 2012 to amend existing contracts with service providers to include personal information security provisions, as long as the existing contracts were entered into before March 1, 2010. As before, service-provider contracts that the company entered into after March 1, 2010, must include personal information security provisions.

Focus on Implementation

The current revision represents what the OCABR considers to be final regulations that will become effective on March 1, 2010. Although the deadline had been extended several times since the initial release, complying with the 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 March 1, 2010.

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