Massachusetts Amends Data Security Regulations and Extends Compliance Deadline

The Data Security Regulations were to be effective as of January 1, 2010, but with this latest amendment the compliance deadline has been extended to March 1, 2010.

The apparent primary purpose of the amendments is to take more of a risk-based approach to security.

On August 17, 2009 the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) announced that it has amended its regulations to protect personal information of residents of the Commonwealth, 201 CMR 17.00 ("Data Security Regulations"). The Data Security Regulations were to be effective as of January 1, 2010, but with this latest amendment the compliance deadline has been extended to March 1, 2010. Although the press release focuses on the effect the Data Security Regulations could have on small businesses, the amendments and extension apply to all businesses that "own or license" personal information about a resident of the Commonwealth. The apparent primary purpose of the amendments is to take more of a risk-based approach to security, which is reflected throughout the revisions. The OCABR has scheduled a hearing on September 22, 2009 at 10:00 a.m. in Room No. 5-6, Second Floor, Transportaion Bldg, 10 Park Plaza, Boston, MA 02116 for interested parties to provide oral or written testimony regarding 201 CMR 17.00 and will accept written comments until the close of business on September 25, 2009 at the offices of the OCABR, 10 Park Plaza, Suite 5170, Boston, MA 02116, Attn: Jason Egan, Deputy General Counsel, or e-mailed to Jason.Egan@state.ma.us.

In its press release and FAQs, the OCABR indicated that a purpose of the amendments was to make clear that the Data Security Regulations, as amended, adopt a risk-based approach to data security, consistent with the Federal Trade Commission's Safeguards Rule. The amendments to the Data Security Regulations address the following: 1) adding consideration of the business' size, scope of business, amount of resources, nature and quantity of data collected or stored and the need for security when creating an information security program; 2) removal of a number of specific provisions that were required, which will now be used as a form of guidance only; 3) specifying that all (not just encryption) computer system security requirements should be included in the written information security program "to the extent technically feasible"; 4) adding and amending definitions, including making the definition of encryption technology neutral.

The definition of "personal information" has remained the same (essentially first name or initial and last name combined with sensitive data like SSN), but new definitions for "own or license" and for "service provider" have been added, both quite broad and should be reviewed. A significant move backwards has occurred with respect to service providers. The amendments have added back in a requirement to impose contractual obligations to maintain appropriate security measures on service providers

If you have any questions about the Massachusetts OCABR Data Security Regulations, please contact the following, or your Vorys relationship attorney:

Benita A. Kahn
bakahn@vorys.com
614.464.6487

with access to or that have use of "personal information." However, if the contract is entered into prior to March 1, 2010, it will be deemed to be in compliance with this obligation until March 1, 2012 even if no such language exists in the contract. Therefore, businesses are given two and a half years notice to amend all service provider contracts that include services which allow access to or use of "personal information."

The amendments do not define "technically feasible," but the FAQs address this concept and define it as whether there is a reasonable means through technology to accomplish a required result. The OCABR further elaborates this in the FAQs by indicating that while it is very clear that there is encryption technology for laptops, they recognize that "at this period in the development of encryption technology, there is little, if any, generally accepted encryption technology for most portable devices, such as such as cell phones, blackberries, net books, iphones and similar devices." The OCABR further warns that if encryption for portable devices is not available, then "personal information" should not be placed on such devices. It should also be noted that while not clearly apparent from the amended rules, the FAQs specify that back up tapes that include "personal information" must be encrypted on a prospective basis.

The amendments have removed some requirements for information security programs. It will no longer be necessary to include in the written program limitations on the amount of "personal information" collected or the length it is retained. Even if not in a written program, these concepts should be considered an important guidance, and certainly remain issues that arise when the FTC reviews the reasonableness of a data security policy. Likewise, it will also no longer be a requirement under the Data Security Regulations to identify in the written program where "personal information" is retained. As the OCABR correctly notes, however, it would be difficult to implement a risk-based data security program without first understanding where the personal information is located.

With the opportunity to submit comments in the next month, these amendments should be reviewed to determine how they will affect all businesses and whether comments should be considered.