Privacy and Security Alert: Analysis of Amendments to Massachusetts Data Security Regulations

8/19/2009

As we reported in our August 17, 2009 Client Alert, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) released amendments to the *Standards to Protect Personal Information of Residents of the Commonwealth*, 201 CMR 17.00 (the Standards). In addition to extending the compliance deadline from January 1, 2010 to March 1, 2010, the amendment makes some key changes that bear taking note of and that we will examine here. The OCABR has scheduled a hearing for interested parties to provide oral or written testimony regarding 201 CMR 17.00 on September 22, 2009 at 10:00 a.m. in Room No. 5–6 on the second floor of the Transportation Building at 10 Park Plaza, Boston. Written comments will also be accepted until the close of business on September 25, 2009 at the offices of the OCABR, 10 Park Plaza, Suite 5170, Boston, Massachusetts, 02116, and should be sent to the attention of Jason Egan, Deputy General Counsel, or e–mailed to Jason.Egan@state.ma.us.

Although the press release from OCABR clearly focused on a beneficial effect to small business, the amendments and extension apply to all businesses that "own or license" personal information of a resident of Massachusetts. Along with its press release, OCABR has also issued a list of FAQs. We have provided a complete text of the FAQs for your convenience here. The agency makes clear that one of the purposes of the amendment was to take a risk–based approach to the Standards, consistent with the Federal Trade Commission's Safeguards Rule. This is familiar territory to those who have been implementing compliance programs under Gramm–Leach–Bliley, Regulation S–P of the Securities and Exchange Commission, any of the Interagency Guidance issued by the bank regulatory agencies, HIPAA, or the Red Flag Rules. The "risk–based approach" in the Standards, as amended, addresses:

1. adding consideration of the size and scope of the business, amount of resources, nature and quantity of data collected or stored, and the need for security when creating an information security program;
2. removing a number of specific provisions for the written information security program, all of which will now be "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 some definitions, including making the definition of encryption "technology–neutral."

According to the OCABR, compliance with the Standards will be judged according to these risk–based factors. There is still no one–size–fits–all written information security plan (WISP) or risk assessment.

Definitions

The definition of "personal information" has remained the same (first name or initial and last name combined with sensitive data like a Social Security number or financial account number). New definitions for "own or license" and for "service provider" have been added, and both are quite broad and should be reviewed.

Service Providers

There has been a significant change with respect to service providers. The current iteration of the Standards contains "due diligence" type language, requiring that businesses use "all reasonable measures" to "ensure" that service providers are "capable" of providing security consistent with the Standards. The amendments delete the "due diligence" requirement, but have added back in a requirement from earlier versions to impose contractual obligations to maintain appropriate security measures on service providers with access to or that use "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." These requirements are consistent with third–party vendor requirements under federal law.

Computer System Requirements

The amendments do not define "technically feasible," but the FAQs address this concept and define it by stating, "if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used." 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 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. The FAQs elaborate on a point that is not readily apparent from the amended Standards, but they have addressed in public outreach seminars: backup tapes that include "personal information" must be encrypted on a prospective basis.

Written Information Security Programs

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 Standards 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. The new FAQs also clarify the following important issues, including the following:

1. Portable devices that contain personal information of Massachusetts residents must be encrypted where it is reasonable and technically feasible to do so. Since little technology exists to reasonably encrypt portable devices other than laptops, businesses should consider restricting sending to and storage of personal information on devices such as Blackberries, PDAs, or USB/thumb drives.
2. An account is a financial account, and thus must be protected under the WISP, if unauthorized access could result in an increase of financial burden or a misappropriation of monies, credit, or other assets.
3. An insurance policy number is a financial account number if it grants access to a person's finances, or results in an increase of financial burden or a misappropriation of monies, credit or other assets.
4. Compliance with HIPAA does not eliminate a company's obligation to comply with the Regulations if the company owns or licenses personal information of a Massachusetts resident.

While the effective date of the Regulations has been postponed to March 1, 2010, there is a considerable amount of work that companies, including many located outside Massachusetts, will need to do to comply.

For assistance in this area, please contact one of the attorneys listed below or any member of your Mintz Levin client service team.

Cynthia Larose, CIPP
(617) 348-1732
CLarose@mintz.com

Dianne J. Bourque
(617) 348-1614
DBourque@mintz.com

Elissa Flynn-Poppey
(617) 348-1868
EFlynn-Poppey@mintz.com

Haydon A. Keitner
(617) 348-4456
HAKeitner@mintz.com

Julia M. Siripurapu
(617) 348-3039
JSiripurapu@mintz.com