Privacy and Security Alert: Massachusetts Revises Data Security Regulations and Gives Three-Month Reprieve for Compliance

8/17/2009

Trying to predict whether a data security regulation will actually become effective is becoming a bit of a party game. The Federal Trade Commission has had the ball rolling with multiple delays of enforcement of its Red Flag identity theft rules. Now, Massachusetts joins in. With its latest amendments to the *Standards for the Protection of Personal Information of Residents of the Commonwealth*, 201 CMR 17.00 (the "Regulations"), Massachusetts is giving businesses until **March 1, 2010** to come into compliance with security safeguards for personal information of Massachusetts residents.

Generally, the Regulations mandate that any entity that stores personal information (a combination of name and Social Security number, bank account number, or credit card number) of Massachusetts residents must encrypt the information when the information is stored on portable devices, or transmitted wirelessly or on public networks. For a detailed description of compliance standards, see our previous alerts (January 22, 2008, October 2, 2008, October 31, 2008, and January 30, 2009). The basic premise has not changed.

What has changed is the approach that the Regulations are taking to the development and implementation of security plans and third party vendor due diligence. According to the press release from the Commonwealth, the amendments to the Regulations strike a balance between maintaining protections on the one hand, and reinforcing flexibility in compliance by small businesses. In particular, the revised regulations take a "risk–based" approach to data security, whereby a business, in developing the required written information security program, may take into account its size, the nature of its business, the kinds of records it maintains, and the risk of identity theft posed by its operations. The previous version of the Regulations targeted the "risk–based" analysis at enforcement only and not at planning. Although the press release seems to focus on "small business," the Regulations are generally applicable, including the three–month extension of time.

New language in the Regulations recognizes that the size of a business and the amount of personal information the business handles play a role in the data security plan the business creates. The new language requires safeguards that are appropriate to the size, scope and type of business handling the information. The revised Regulations also take into consideration the amount of resources available to a business, the amount of data the business stores, and the need for security and confidentiality of consumers' and employees' personal information. These are similar to "safeguards" language found in federal law, including the Gramm–Leach–Bliley Act and the Red Flag Identity Theft Rules.

Consistent with the more flexible approach under the revised Regulations, a number of specific provisions required to be included in a business's written information security program have been removed from the Regulations and will be used as a form of guidance only. In addition, the Regulations, as amended, are technology neutral and acknowledge that technical feasibility plays a role in what many businesses, especially small businesses, can do to protect data. Lastly, third party vendor requirements have been changed to be consistent with federal law.

The full text of the amended Regulations can be found here. The Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) today sent to the Secretary of State notice of public hearing on the changes. That hearing will be held on Tuesday, September 22, at 10 a.m. at the Transportation Building, 10 Park Plaza, Boston.

Any company holding personal information of Massachusetts residents should become familiar with the Regulations' provisions in order to comply with the requirements prior to the effective date of March 1, 2010. Mintz Levin's Data Security Group can serve as a resource. Our attorneys have extensive experience in assisting clients with regulatory compliance in volatile environments. Should you have any questions, feel free to contact us.

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

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