Shipman & Goodwin LLP

Security Alert

December 2008

NOTE: Massachusetts extended deadline for compliance to January 1, 2010; revised certain requirements: The Massachusetts Office of Consumer Affairs and Business Regulation recently extended the compliance date for the regulations outlined below to January 1, 2010. Also, the regulations were revised to remove the requirement that entities obtain written certification from third party providers with access to personal information that the third party providers have a written information security program consistent with the regulations. Now, under the revision, entities that possess personal information of Massachusetts residents are to take reasonable steps to (1) verify that a third party service provider with access to such personal information has the capacity to protect the personal information in the manner provided for in the regulations; and (2) ensure that such third party service provider is applying to the personal information protective security measures at least as stringent as required in the regulations.

NEW MASSACHUSETTS REGULATIONS SET HIGH STANDARDS FOR PERSONAL INFORMATION PROTECTION

GENERAL COMPLIANCE DEADLINE EXTENDED FROM JANUARY 1, 2009 TO MAY 1, 2009.

Recently, the Massachusetts Office of Consumer Affairs and Business Regulation adopted regulations for the protection of Personal Information of residents of Massachusetts. Effective May 1, 2009, the regulations (201 CMR 17.00) apply to persons that own, license, store or maintain Personal Information of residents of Massachusetts. **Thus, the new regulations could apply, for example, to organizations doing business in Connecticut who have employees or contractors who are Massachusetts residents; organizations doing business in Connecticut who store and maintain the Personal Information of customers who are Massachusetts residents; or organizations doing business in Connecticut who store and maintain for others the Personal Information of Massachusetts residents**. These new regulations do not explicitly limit compliance to entities doing business in Massachusetts. The regulations are the most comprehensive in the country to date and may become the "gold standard" that everyone will have to meet.

WHAT IS "PERSONAL INFORMATION"?

Personal Information is the person's first (or first initial) and last name coupled with the person's Social Security number, driver's license number, state-issued ID number, or financial account/ credit/debit card number (with or without an access code). There are exceptions for personal information obtained from public sources. However, the exceptions aren't sufficiently broad to excuse general compliance with the mandates of the regulations.

COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM.

For all who have Personal Information of Massachusetts residents, the regulations require the creation of a comprehensive written information security plan ("WISP") that must be adopted, monitored, and periodically updated. The WISP must describe the administrative, technical and physical safeguards implemented to protect the Personal Information contained in both paper and electronic records. For many, this may require system changes, updated security (physical and electronic) measures, more extensive use of encryption, and new training and monitoring programs.

ENCRYPTION OF PERSONAL INFORMATION.

As noted above, the regulations require more extensive use of encryption to protect Personal Information, including (1) to the extent feasible, encryption of all transmitted electronic records and files containing Personal Information that travel across public networks and all data that is to be transmitted wirelessly; and (2) encryption of all Personal Information stored on laptops or other portable electronic devices. While the compliance deadline for encryption of laptops was extended to May 1, 2009, the deadline for encryption of other portable devices was further extended to January 1, 2010.

THIRD PARTY SERVICE PROVIDERS.

The new regulations also impose obligations on entities that give access to Personal Information to third party service providers. If a third party service provider is given access to Personal Information, the entity must take reasonable steps to ensure that the provider has the capacity to maintain safeguards to protect the Personal Information and must obtain a written certification from the third party service provider that it has a written, comprehensive information security program in compliance with these regulations. This will almost certainly require that a written agreement drafted to comply with the new regulations be put in place between the entity giving access to the Personal Information of Massachusetts' residents and the third party service company. While the compliance deadline for ensuring that third party providers are capable of protecting Personal Information and contractually binding them to do so was extended to May 1, 2009, the deadline for requiring written certification from third party providers was further extended to January 1, 2010.

RELATED LAW REGARDING DISPOSAL OF PERSONAL INFORMATION.

A related Massachusetts law already in effect as of February 3, 2008 (General Laws of Massachusetts Chapter 93I) establishes minimum standards for the proper disposal of records containing Personal Information. These standards include physical shredding and other secure disposal methods in lieu of "reversible" erasure. Proper tracking, control and disposal of physical and electronic copies are an important part of an effective disposal policy and should also be included in the WISP.

QUESTIONS OR ASSISTANCE?

If you have any questions about collection, safeguards and disposal plans for personal information, how to plan effectively to limit the risk of a personal information data breach, or how to deal with a breach if it should occur, please feel free to contact John Kreitler at (860) 251-5119 (jkreitler@goodwin.com) or Catherine Intravia at (860) 251-5805 (cintravia@goodwin.com).

SHIPMAN & GOODWIN LLP®

COUNSELORS AT LAW

One Constitution Plaza
Hartford, CT 06103-1919
(860) 251-5000

300 Atlantic Street
Stamford, CT 06901-3522
(203) 324-8100

289 Greenwich Avenue
Greenwich, CT 06830-6595
(203) 869-5600

12 Porter Street
Lakeville, CT 06039-1809
(860) 435-2539

www.shipmangoodwin.com