Deadline for Complying with Massachusetts' New Personal Data Security Law Fast Approaching

By Joseph T. Bartulis, Jr., Esq.

As you may know, Massachusetts passed a comprehensive data security law and related regulations which must be complied with by all businesses that maintain "personal information" of its employees, customers, or vendors, etc. While the deadline for compliance has been pushed back three times, it is presently scheduled to go into effect March 1, 2010. It is unanticipated that the effective compliance date will be pushed back any farther.

The new law and its attendant regulations impose minimum standards for safeguarding personal information contained in both paper and electronic records. The law and the regulations are meant to greatly diminish the risk of one's personal information being compromised by creating a significant onus on the possessors of such information to safeguard it. The regulations were promulgated by the Commonwealth's Office of Consumer Affairs and Business Regulation and are contained in the Code of Massachusetts Regulations at 201 CMR 17.00.

Personal information is defined as a Massachusetts resident's first name and last name or first initial and last name in combination with the resident's: (a) Social Security number; or (b) driver's license number; or (c) a financial account number or credit card number. Businesses that fail to take the necessary steps to safeguard this personal information will, if a breach occurs, be subjected to potential civil penalties of $5,000 for each violation, among other things.

KEY ELEMENTS OF THE REGULATIONS

At its core, there are two main areas that must be addressed to protect one's organization from significant potential liability. They are: protection of the data generally (via what is referred to in the regulations as a Written Information Security Program "WISP") and through the implementation and use of certain computer system information technology protections and practices. In this article, I will very briefly highlight the key items of the WISP document.

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

Whether an organization has taken appropriate steps in its WISP to protect information shall be evaluated by taking into account: "(i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (ii) the amount of resources available to such person; (iii) the amount of stored data; and (iv) the need for security and confidentiality of both consumer and employee information."

Each WISP must address the following points: It should: 1) specifically name one or more designated individuals as the overseer of the organization's protection of personal information; 2) identify risks & assess current safeguards; 3) contain policies regarding whether and how employees may keep, access, and transport records containing personal information off of business premises; 4) contain statements that employees will be subject to discipline measures for violations of the WISP; 5) bar access by former employees the moment they leave your organization' employ; 6) contain a statement that the organization will take reasonable steps to verify that third-party service providers that the organization allows access to personal information (e.g. credit card processor) have the capacity to protect such personal information; 7) specify that personal information should only be retained for the minimum amount of time needed to complete the transaction for which it was provided; (8) detail the process by which the organization identifies paper, electronic and other records, including laptops and portable devices which contain personal information; 9) establish written procedures to restrict physical access to records; 10) contain language that the "designated employee" will regularly monitor the organization's personal information practices to confirm whether the organization is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; 11) contain a statement that, in addition to the regular monitoring (see #10), the organization's designated employee will also conduct a thorough review of the WISP no less often than annually; and 12) contain a procedure to document breaches that occur and what responsive actions will be/were taken.

MARCH 1ST DEADLINE WILL BE HERE SOON

The deadline for preparing a WISP and complying with the new regulations is less than ninety days away. Your organization should promptly take steps to prepare a WISP which addresses each of the above items and to make sure your IT department has taken all of the requisite IT steps required under the regulations (which were not discussed in this short article but can be found in 201 CMR 17.00) as well.

RESPONSIVE SOLUTIONS

Two simple words that explain our commitment to you. Being responsive is a critical element in building a strong attorney-client relationship. Whether you are a new or existing client, we'll be quick to respond to your needs with the knowledge necessary to find solutions to your legal concerns.

Joseph T. Bartulis, Jr., Esq., is an officer with the firm and is Chairperson of its Labor and Employment Law Practice Group. Mr. Bartulis advises employers on all aspects of the employer-employee relationship and would be happy to assist your business. He can be reached at 508-459-8214 and at jbartulis@fletchertilton.com.

www.fletchertilton.com

Joseph T. Bartulis, Jr.
P: 508.459.8214
F: 508.459.8414
E: jbartulis@fletchertilton.com

Fletcher Tilton PC
Attorneys at law

THE GUARANTY BUILDING
370 Main Street, 12th Floor
Worcester, MA 01608
TEL 508.459.8000 FAX 508.459.8300

THE MEADOWS
161 Worcester Road, Suite 501
Framingham, MA 01701
TEL 508.532.3500 FAX 508.532.3100

CAPE COD
1579 Falmouth Road, Suite 3
Centerville, MA 02632
TEL 508.815.2500 FAX 508.459.8300