Massachusetts Adopts Data Security Regulations

Massachusetts has enacted detailed data security regulations that will apply to anyone who owns, licenses, stores or maintains "personal information" about a Massachusetts resident and require compliance by January 1, 2009.

In an ongoing state response to the TJX data compromise, the Massachusetts Department of Consumer Affairs and Business Regulation recently issued data security regulations. While federal laws affecting various industries and many states have enacted data security requirements, to date these have been somewhat generic, requiring administrative, technical and physical safeguards. In 2007, Minnesota enacted legislation that was more specific, addressing the protection of magnetic stripe data on credit and debit cards. The Minnesota law imposes liability on merchants who have a security breach involving magnetic stripe data that is retained for more than 48 hours after authorization.

Massachusetts has taken this one step further by enacting regulations with detailed requirements for the protection of "personal information". While companies faced with PCI compliance have addressed many of these protections for credit card information, they may not have addressed these requirements as they relate to social security numbers. The following summarizes the applicability and obligations under these new requirements:

Applicability: Applies to all persons or entities that own, license, store or maintain personal information about a Massachusetts resident. This applies to both paper and electronic records. This will affect companies that have employees/associates who are residents of Massachusetts and possibly could affect companies that store or maintain "personal information" about customers who are residents of Massachusetts.

Effective Date: January 1, 2009.

Personal Information Affected: "Personal information" is defined as an individual's name **in combination with** his or her Social Security number, driver's license number, financial account number, or credit or debit card number.

Security Program Requirements (paper and electronic records with "personal information"):

General Requirement: For records containing "personal information," develop, implement, maintain and monitor a comprehensive, written information security program that is consistent with industry standards, taking into account the size, scope and type of business, the amount of resources available to the business, and the amount of stored data.

Specific Requirements: The regulations also require implementation of the following specific safeguards, most of which have not been a part of explicit security requirements under previous state data security programs (although some may have been implied):

Appointing one or more employees to maintain the information security program;

- Limiting the amount and time of retention of "personal information" to what is necessary to achieve the purpose for which is collected;
- Ongoing employee training and disciplinary measures for violation of the program;
- Addressing access from the perspective of how employees should be allowed to keep, access and transport records

If you have any questions, please contact one of the following, or your Vorys relationship attorney:

Benita A. Kahn
614.464.6487

W. Breck Weigel
513.723.4078

with "personal information," how to prevent terminated employee access and limiting physical access (locked facilities, storage areas or containers);

- Implementation of intrusion detection and intrusion prevention (for paper and electronic records);
- Identifying paper and electronic records, computing systems, storage media (including laptops and portable devices) where "personal information" is stored;
- Contractually requiring service providers to properly protect "personal information." This includes obtaining written certification from service providers that they have a compliant written information security program;
- Documenting responsive actions to a breach of "personal information" and post-incident review; and
- Reviewing the information security program annually and revising as necessary to limit risks.

Computer System Security Requirements (electronic storage or transmission): Specific requirements for electronically stored or transmitted "personal information" are also included and require the following, at a minimum:

- To the extent technically feasible, encryption of all "personal information" that will travel over public networks, encryption of all data transmitted wirelessly;
- Encryption of all "personal information" stored on laptops or other portable devices;
- Secure authentication protocols - control of user IDs, a secure method of assigning passwords, blocking access to user identification after multiple attempts and restricting access to active user accounts;
- Secure access control measures that restrict access to "personal information" to those with a need-to-know and assign unique passwords that are not vendor supplied;
- Monitoring of systems for unauthorized use or access to "personal information";
- Up to date firewall protection and up to date patches and virus definitions (including anti-virus software with malware protection); and
- Employee training on the proper use of the computer security system and the importance of data security.

Enforcement: These regulations were promulgated under the Massachusetts breach notification law, Chapter 93H, which went into effect October 31, 2007. This statute authorizes the Massachusetts Attorney General to bring actions for violations of this law pursuant to its authority under Massachusetts' consumer protection law. The Massachusetts Attorney General may seek injunctive relief and, in some instances, civil penalties.