

Changes Coming for Customer Personal Data

Is Your Company in Compliance?

By **Melissa J. Krasnow**

Nevada was the first state to enact a law requiring entities that transfer customer personal information outside of the secure system of the business through an electronic transmission (other than a facsimile) to use encryption. In late 2008, Massachusetts was the second state to pass legislation that mandates the use of encryption. Michigan is considering similar legislation. This is an area to watch as other states could consider such legislation.

The Massachusetts legislation goes beyond encryption, also requiring entities to develop, implement, maintain and monitor a comprehensive, written information security program on or before Jan. 1, 2010. This article describes the application of and the compliance requirements for the first-of-its kind Massachusetts regulation issued by the Massachusetts Office of Consumer Affairs and Business Regulation ("MOCABR").

APPLICATION

This regulation has broad reach, applying to each person or entity that owns, licenses, stores or maintains personal information about a Massachusetts resident ("Covered Entity"). "Personal information" means a Massachusetts resident's first and last name or first initial and last name in combination with a: 1) Social Security Number; 2) driver's license or state-issued identification card number; or 3) financial account number. According to the MOCABR, this regulation is not preempted if an entity complies with the

Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act requirements.

COMPREHENSIVE, WRITTEN INFORMATION SECURITY PROGRAM

A Covered Entity must be in full compliance with this regulation on or before Jan. 1, 2010, including developing, implementing, maintaining and monitoring a comprehensive, written information security program applicable to records containing personal information ("Program").

A Covered Entity must

be in full compliance

with this regulation on

or before Jan. 1, 2010

Standards and Safeguards

This regulation establishes minimum standards to meet in connection with the safeguarding of personal information in paper and electronic records. The Program must be reasonably consistent with industry standards and contain administrative, technical and physical safeguards to ensure the security and confidentiality of these records. The safeguards in the Program must be consistent with the safeguards for protection of personal information and information of a similar character in any state or federal regulations to which the Covered Entity is subject. To determine whether the Program is compliant, the following factors must be considered: 1) the size, scope and type of business of the

Covered Entity; 2) the amount of resources available to the Covered Entity; 3) the amount of stored data; and 4) the need for security and confidentiality of both consumer and employee information.

Requirements

The Program must do the following:

1. Designate one or more employees to maintain the Program;
2. Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality or integrity of any records containing personal information, and evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting these risks (e.g., ongoing temporary, contract and regular employee training, employee compliance with policies and procedures and means for detecting and preventing security system failures);
3. Develop security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises;
4. Impose disciplinary measures for violations of the Program;
5. Prevent terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to these records (e.g., deactivating their passwords and user names);
6. Take all reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect this personal information in the manner provided for in this regulation; and ensure that these third-party service providers are applying personal information protective security measures at least as stringent as those required to be applied to personal information under this regulation;

7. Limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected, limit the time personal information is retained to that reasonably necessary to accomplish this purpose and limit access to those persons who are reasonably required to know personal information to accomplish this purpose or to comply with state or federal record retention requirements;

8. Identify records, computing systems, and storage media (e.g., laptops and portable devices used to store personal information) to determine which records contain personal information, except where the Program provides for the handling of all records as if they all contained personal information;

9. Implement reasonable restrictions on physical access to records containing personal information (including a written procedure regarding the manner in which physical access to these records is restricted) and store the records and data in locked facilities, storage areas or containers;

10. Regularly monitor to ensure that the Program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and upgrade information safeguards as necessary to limit risks;

11. Review the scope of the security measures at least annually or when there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information;

12. Document responsive actions taken when a data security breach incident occurs and conduct a mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to the protection of personal information; and

13. Establish and maintain a security system, covering its computers and any wireless system, for a Covered Entity that electronically stores or transmits personal information, which, at a minimum:

(A) secures user authentication protocols, including: 1) control of user IDs and other identifiers; 2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies

(e.g., biometrics or token devices); 3) control of data security passwords to ensure that these passwords are kept in a location or format that does not compromise the security of the data they protect; 4) restricting access to active users and active user accounts only; and 5) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(B) has secure access control measures that: 1) restrict access to records and files containing personal information to those who need personal information to perform their job duties; and 2) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(C) to the extent technically feasible, encrypts (i.e., transforms data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key) all transmitted records and files containing personal information that will travel across public networks, and encrypts all data to be transmitted wirelessly;

(D) has reasonable monitoring of systems for unauthorized use of or access to personal information;

(E) encrypts all personal information stored on laptops or other portable devices;

(F) includes reasonably up-to-date firewall protection and operating system security patches for files containing personal information on a system that is connected to the Internet, reasonably designed to maintain the integrity of the personal information;

(G) has reasonably up-to-date versions of system security agent software, which includes malware protection and reasonably up-to-date patches and virus definitions or a version of this software that can still be supported with up-to-date patches and virus definitions, and is set to

receive the most current security updates on a regular basis; and (H) educates and trains employees on the proper use of the computer security system and the importance of personal information security.

ENFORCEMENT

The statute under which this regulation was issued provides for enforcement by the Massachusetts Attorney General. The MOCABR stated in its "Frequently Asked Qs" that it will discover "who is not playing by the rules when a [data security] breach occurs and it is investigated."

NEXT STEPS

Given the broad application of this regulation and the compliance date of Jan. 1, 2010, an entity needs to determine whether it is a Covered Entity. If so, the Covered Entity must work on preparing and implementing a Program. As part of this Program, the Covered Entity must take all reasonable steps to verify that third-party service providers have the capacity to protect personal information in the manner provided for in this regulation and to ensure that they are applying personal information protective security measures at least as stringent as those required to be applied to personal information under this regulation. Also, the Covered Entity must, to the extent technically feasible, encrypt all transmitted records and files with personal information that will travel across public networks, and encrypt all data to be transmitted wirelessly. Finally, the Covered Entity must encrypt all personal information stored on laptops or other portable devices.