

Compliance Programs

Financial Services

Final Massachusetts Privacy Regulation: What Is Required and How to Comply

Contributed by: Melissa J. Krasnow, Dorsey & Whitney LLP

The Massachusetts Office of Consumer Affairs and Business Regulation ("MOCABR") recently issued the final version of the Massachusetts privacy regulation (Regulation).¹ This article provides a summary of this Regulation, which applies to each person or entity that owns or licenses personal information about a Massachusetts resident (Covered Entity).² "Owns or licenses" means receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment. "Personal information" means a Massachusetts resident's first and last name or first initial and last name in combination with a (i) Social Security Number; (ii) driver's license or state-issued identification card number or (iii) financial account number.³ According to the MOCABR, this Regulation is not preempted if a Covered Entity complies with the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act requirements. Consequently, this Regulation could apply to any type of business.

A Covered Entity must be in full compliance with this Regulation on or before March 1, 2010, including developing, implementing and maintaining a comprehensive, written information security program applicable to records containing personal information (Program).⁴

This Regulation establishes minimum standards for safeguarding personal information in paper and electronic records.⁵ The Program must be written in one or more readily accessible parts and contain administrative, technical and physical safeguards 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 may be regulated.

The safeguards must be appropriate to (i) the size, scope and type of business of the Covered Entity; (ii) the amount of resources available to the Covered Entity; (iii) the amount of stored data and (iv) the need for security and confidentiality of both consumer and employee information.⁶

The Regulation requires a Covered Entity to take the following action:

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 electronic, paper or other 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 relating to the storage, access and transport of 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;
6. Take reasonable steps to select and retain third-party service providers (i.e., any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a Covered Entity) that are capable of maintaining appropriate security measures to protect such personal information consistent with this Regulation and any applicable federal regulations;
7. Require third-party service providers by contract to implement and maintain appropriate security measures for personal information (though a contract a Covered Entity has entered into no later than March 1, 2010 with a third-party service provider satisfies this provision even if the contract does not include a requirement that the third-party service provider maintain such appropriate safeguards, until March 1, 2012);
8. Implement reasonable restrictions on physical access to records containing personal information and store the records and data in locked facilities, storage areas or containers;
9. 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;
10. 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;

11.

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

12.

Establish and maintain a security system, covering its computers and any wireless system, for a Covered Entity, which, at a minimum and to the extent technically feasible (i.e., if there are reasonable means through technology to accomplish a required result):

a.)

secures user authentication protocols, including (i) control of user IDs and other identifiers; (ii) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies (e.g., biometrics or token devices); (iii) 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; (iv) restricting access to active users and active user accounts only and (v) blocking access to user identification after multiple unsuccessful attempts to gain access or limiting access for the particular system;

b.)

has secure access control measures that (i) restrict access to records and files containing personal information to those who need personal information to perform their job duties and (ii) 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.)

encrypts (i.e., transforms data 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.⁷

The statute under which this Regulation was issued provides for enforcement by the Massachusetts Attorney General.⁸

Companies that are developing or have developed comprehensive, written information security programs need to revisit what they have done thus far to make sure it complies with the Regulation, and whether it is subject to the Nevada encryption law. Under the Nevada encryption law, a company (except for a telecommunications provider) doing business in Nevada that deals with personal information must comply with specific encryption requirements if it does not accept a payment card (a credit card or similar card) in connection with a sale of goods or services. This law also requires that a company that does accept payment cards in connection with a sale of goods or services comply with the current version of the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an industry security standard developed by the PCI Security Standards Council (including American Express, Discover, JCB, MasterCard and Visa) for the protection of customer account data. The compliance deadline for the Nevada encryption law is January 1, 2010.⁹

Other companies immediately need to determine whether they are covered by the Regulation. Their compliance efforts should begin now if they determine that they are covered.

Finally, companies that determine that they are not covered typically prepare a written summary of their determination.

Melissa J. Krasnow is a partner in the Corporate Group of Dorsey & Whitney LLP.

1
201 CMR 17.00.

2
[Id. at 17.01\(2\).](#)

3
[Id. at 17.02.](#)

4
[Id. at 17.05.](#)

5
[Id. at 17.01\(1\).](#)

6
[Id. at 17.03\(1\).](#)

7
[Id. at 17.03\(2\) and 17.04.](#)

8
See Mass. Gen. Laws ch. 93H.

9

Nev. S.B. No. 227.

Legal Topics:

[Compliance Programs](#)

[Financial Services](#)

[Disclaimer](#)

The discussions set forth in this report are for informational purposes only. They do not take into account the qualifications, exceptions and other considerations that may be relevant to particular situations. These discussions should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content contained in this report and do not make any representation or warranty as to its completeness or accuracy.

©2009 Bloomberg Finance L.P. All rights reserved. Bloomberg Law Reports[®] is a registered trademark and service mark of Bloomberg Finance L.P.