Client Alert

pillsbury

Privacy & Data Protection | Global Sourcing
Consumer & Retail | Travel, Leisure & Hospitality
Restaurant, Food & Beverage | Financial Services

November 12, 2008

New Massachusetts Regulation Requires Comprehensive Written Information Security Program from Businesses by January 1, 2009

by Catherine D. Meyer, John L. Nicholson and Meighan E. O'Reardon

The Massachusetts Office of Consumer Affairs & Business Regulation recently published a regulation to implement the provisions of Massachusetts General Law chapter 93H, its security breach statute. Businesses holding personal information about Massachusetts residents must (1) develop a written plan and appoint an employee to manage it and enforce violations, (2) implement fire-walls and encrypt information in transit and on portable devices, and (3) train employees on information security. The regulation applies to all entities that own, license, store or maintain personal information about a resident of Massachusetts and goes into effect January 1, 2009.

The Massachusetts regulation imposes a duty to protect personal information and provides administrative standards as well as computer system security requirements. Administratively, each entity holding personal information is required to enact a comprehensive **written** information security program compliant with the regulations that must include, among other things, identification of risks and development of safeguards against those risks, policies addressing access and transportation of records, disciplinary consequences for violation of the program, vendor oversight, physical, administrative and electronic limitations on access to personal information (such as through the use of passwords, locked facilities, etc.), limitations on the amount of information collected and the length of time it is maintained, and mechanisms to monitor and update the program.[1]

Background

Massachusetts enacted a security breach statute, effective October 2008, that imposes a duty on anyone owning or licensing personal information to develop, implement, maintain and monitor a comprehensive,

[1] 201 Mass. Code Regs. 17.03 (2008).

written information security program to ensure the integrity of the information and to protect against unauthorized access that could result in harm.[2] The Massachusetts Office of Consumer Affairs & Business Regulation has adopted OCABR Regulation 17.00 to address implementation of the statutory directive. Massachusetts, by statute, **requires** protection of personal information, but moves a step further from the generally described requirement of "reasonable security measures" to a specific regulation imposing **minimum** compliance standards.

The Purpose and Requirements of the Regulation

The stated purpose of the regulation is to establish "minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. Further purposes are to (i) ensure the security and confidentiality of such information in a manner consistent with industry standards, (ii) protect against anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud against such residents."[3]

The regulation imposes a duty to protect personal information. It outlines computer system security requirements including use of security protocols for user authentication, controls and restrictions on access to the information, monitoring for unauthorized use of the system, malware protection programs, encryption of all personal information on laptops or other portable devices (which would likely include CDs, DVDs, flash drives, etc.), and encryption of all transmitted records traveling across public networks or wirelessly.[4]

Businesses that hold information about Massachusetts residents must develop, maintain, and enforce a written information security plan, appropriate to the size and complexity of the organization, that meets basic criteria including:

1. Designating one or more employees charged with maintaining the program.

2. Identifying reasonably foreseeable risks (internal and external) to the security of the organization's records containing personal information and evaluating and improving the effectiveness of the safeguards currently in place for limiting those risks, including staff training, overall compliance, detection and prevention of system attacks or failures.

3. Developing policies for keeping, accessing and transporting records containing personal information outside the business premises.

4. Establishing disciplinary measures and procedures.

5. Excluding terminated employee access to systems.

6. Oversight of third parties who have access to the personal information to ensure their protection of the data and compliance with the Regulation.

7. Limiting the amount of information collected, the time it is maintained, and access to the information.

[2] Mass. Gen. Laws. ch. 93H, § 2 (2007).

[3] 201 Mass. Code Regs. 17.01(a) (2008).

[4] *Id.*

8. Identifying all devices and media that store personal information.
9. Restricting physical access to the records.
10. Monitoring compliance.
11. Annually reviewing the program and its effectiveness.
12. Documenting responses to any security breach incident.

The regulation applies to all entities that own, license, store or maintain personal information about a resident of Massachusetts.[5] Thus, like other security breach notification statutes, this regulation is resident-centric and ignores the location of the business or person holding the personal information.

Definitions

Massachusetts defines "personal information" as "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account" but not including publicly available information.[6]

Massachusetts expands the scope of the "records" that are protected to include any format on which information (written, drawn, spoken, visual or electromagnetic) is preserved or recorded.[7]

The statute defines "encryption" to require the use of a 128-bit or higher algorithmic process, unless further defined by the regulations. This makes the statute unusual among similar state laws by specifying a specific level of encryption. The regulation employs a more general description (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").[8]

Enforcement

The Massachusetts Attorney General may bring an action to remedy violations of this statute and regulation. In addition, oversight is provided by the Office of Consumer Affairs and Business Regulation. At this time it is uncertain whether companies operating outside Massachusetts, but holding information about Massachusetts residents, will be subject to enforcement actions. Therefore, companies outside Massachusetts who hold information about Massachusetts residents are at risk of potential enforcement if they fail to comply with these regulations. The Massachusetts Attorney General is currently studying enforcement procedures.

[5] *Id.* at 17.01(b).
[6] *Id.* at 17.02
[7] *Id.*
[8] *Id.*

Implications

To date, many data protection laws have been focused on breach notification and the response to security failures. The Massachusetts regulation is significant because it represents a trend toward states taking proactive steps focused on preventing data breaches and security incidents. Some analysts have noted that the new Massachusetts regulation, and other similar state laws, may be used by courts to define the minimum duty that businesses owe to individuals to protect sensitive data. As security standards set forth in these state regulations become increasingly common, a breach of such standards could be used by courts to support civil lawsuits against holders of compromised data. This may be true even if the compromised data is not the type typically protected under a particular state's laws.

Suggested Compliance Review

Businesses with national operations, and especially those doing business or planning to do business in Massachusetts and those with a national customer or employee database, should be apprised of the new Massachusetts regulations. Such businesses should review their information security policies and procedures to confirm that they are in compliance with the statutes and regulations and not in inadvertent violation. Businesses in other jurisdictions would be well advised to watch for the development of similar laws in their respective states.

Significantly, the Massachusetts regulation applies to any entity that stores or uses information about a resident, meaning a presence in Massachusetts is not required to be liable under the regulation. Businesses must be aware not only of the types of personal information they collect but also to whom that information relates. Ultimately, anyone who regularly deals with personal information will need to assess whether they hold Massachusetts residents' information. Given the current public sensitivity to data security, non-Massachusetts-based businesses should consider incorporating the Massachusetts requirements into their information security programs.

In response to the countless data breaches involving lost or stolen laptops, the regulation requires businesses to encrypt personal information stored on portable devices. As such, businesses should review their electronic security policies and procedures. Compliance with this requirement means equipping laptops and other similar devices with encrypted hard drives or installing data encryption software to protect sensitive data. The Commonwealth of Massachusetts estimates that the initial compliance cost for small businesses will be approximately $3,000 for every 10 employees, and companies should budget an additional $500 a month afterward for every 10 employees.[9] Larger companies anticipate allocating similar amounts toward compliance.[10]

The regulation also requires businesses to take a closer look at outsourcing arrangements. In particular, businesses must verify that third-party service providers with access to personal information about Massachusetts residents have the capacity to protect that data. This includes "contractually requiring service providers to maintain such safeguards."[11] At a minimum, businesses that may collect Massachusetts residents' personal information, or are in the business of regularly collecting personal information, should revisit existing outsourcing agreements to verify that compliance by the provider is addressed. If not, businesses should amend any agreements that do not provide adequate information security provisions to

[9] Ben Worthen, "New Data Privacy Laws Set for Firms," *Wall Street Journal* (October 16, 2008).

[10] *Id.*

[11] 201 Mass. Code Regs. 17.03(f) (2008).

comply with the Massachusetts regulation. Going forward, all new outsourcing agreements should include provisions for compliance by the service provider.

Finally, businesses should be aware that the Massachusetts regulation applies not only to electronic records, but also to personal information stored on paper. As such, a review of both electronic and physical storage policies and procedures may be warranted.

For further information, please contact:

Catherine D. Meyer (bio)
Los Angeles
+1.213.488.7362
catherine.meyer@pillsburylaw.com

Deborah S. Thoren-Peden (bio)
Los Angeles
+1.213.488.7320
deborah.thorenpeden@pillsburylaw.com

Wayne C. Matus (bio)
New York
+1.212.858.1774
wayne.matus@pillsburylaw.com

John L. Nicholson (bio)
Washington, DC
+1.202.663.8269
john.nicholson@pillsburylaw.com

Meighan E. O'Reardon (bio)
Washington, DC
+1.202.663.8377
meighan.oreardon@pillsburylaw.com