JONES DAY

FEBRUARY 2010

MASSACHUSETTS LAW RAISES THE BAR FOR DATA SECURITY

On March 1, 2010, what is widely considered the most comprehensive data protection and privacy law in the United States—201 C.M.R. 17: Standards for the Protection of Personal Information of Residents of the Commonwealth (the "Massachusetts Standards")—will take effect. This regulation issued by the Department of Consumer Affairs and Business Regulation pursuant to Massachusetts General Law Chapter 93H will require every business that licenses or owns personal information of Massachusetts residents to comply with the minimum security standards set forth in the regulation. Although a number of states have enacted legislation that mandates the protection of personal information, the Massachusetts Standards are the most onerous of the state data security regulations and will be the "gold standard" going forward. Many of the data security regulations of these other states do not even prescribe the standards of security beyond meeting a reasonable standard or what is appropriate to the nature of the information. However, the Massachusetts Standards not only detail the specific elements that each business's information security program should contain, but go one step further to require, where technically feasible, the encryption of personal information stored on portable devices and personal information transmitted across public networks or wirelessly. The floor for data security standards for Massachusetts-based companies and companies that maintain personal information about Massachusetts residents will be set by the Massachusetts Standards.

STANDARDS FOR PROTECTING PERSONAL INFORMATION

The Massachusetts Standards require any natural person or entity (excluding the Massachusetts government and any natural person not engaged in commerce) that owns or licenses personal information of a Massachusetts resident to implement a written information security program ("WISP") with appropriate administrative, technical, and physical safeguards.[1] Such safeguards must be consistent with

those set forth in state and federal regulations to which a business is subject, including data breach notification laws, HIPAA, and the Gramm-Leach-Bliley Act.

The Massachusetts Standards define "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." The Massachusetts Standards exclude from the definition any information lawfully obtained from publicly available information or from government records available to the general public.[2]

The Massachusetts Standards adopt a risk-based approach to information security, meaning that a business should take into account "the particular business'[s] size, scope of business, amount of resources, nature and quantity of data collected or stored, and the need for security" in implementing its WISP.[3] The regulation does not prescribe a one-size-fits-all approach and allows small businesses that do not store or transfer large amounts of personal information to adopt less stringent requirements in their WISPs.

WRITTEN INFORMATION SECURITY PROGRAM REQUIREMENTS

The Massachusetts Standards set forth the following specific requirements that each WISP should contain:

1. The designation of at least one employee to maintain the WISP;
2. The assessment of risks to the security of records containing personal information, and improvement of safeguards to mitigate such risks, including employee training and detection and prevention of security system failures;
3. Disciplinary measures for violations of the WISP and safeguards for preventing terminated employees from accessing records containing personal information;
4. The development of security policies for the storage, access, and transportation of records containing personal information outside of business premises;
5. The implementation of reasonable restrictions upon physical access to records containing personal information, and the storage of such records and data in locked facilities, storage areas, or containers;
6. Monitoring the WISP's effectiveness in preventing unauthorized access to or use of personal information;
7. The review of the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably affect the security or integrity of records containing personal information; and
8. The documentation of responsive actions to any security breach incidents and of post-incident review of events and actions taken to change business practices.[4]

In addition, businesses are required to limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected and to limit the time such information is retained to that reasonably necessary to accomplish such purpose.[5]

COMPUTER SYSTEM SECURITY REQUIREMENTS AND DATA ENCRYPTION

Each business's WISP must also establish a computer security system with minimum standards for information security protocols "to the extent technically feasible." The term "technically feasible" means that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.[6] The information security protocols that must be implemented, if technically feasible, include:

1. Secure control of user identifiers and passwords for authentication purposes;

2. Lock-out processes for inactive users or unsuccessful log-in attempts;
3. Limiting access to personal information to those persons who are reasonably required to know such information;
4. Up-to-date firewall protection and operating system security patches for systems connected to the Internet;
5. Up-to-date versions of system security agent software, including malware protection, patches, and virus definitions; and
6. Education and training of employees on the proper use of the computer security system.[7]

However, the most significant of these protocols is the requirement to encrypt, where technically feasible, all records and files containing personal information that are transmitted across public networks or wirelessly and all personal information stored on laptops or other portable devices, including backup tapes, on a prospective basis (and existing tapes being transported, if possible).[8] Although Nevada has also adopted regulations that require encryption of transmitted and stored personal information, the scope of the requirement in the Massachusetts regulation is broader than that of Nevada's. The Nevada regulation mandates encryption of personal information on data storage devices that are moved beyond the logical or physical controls of the business, while the Massachusetts Standards require encryption of personal information on portable devices even if such devices do not leave the premises of the business.[9] Both regulations obligate businesses to encrypt personal information when transmitted outside the secure systems of the businesses, but the Massachusetts Standards also require encryption of any personal information transmitted wirelessly in any location.[10]

The Massachusetts Standards define "encrypted" as "transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key."[11] The data must be altered into an unreadable form, and mere password protection does not meet this requirement.[12] Any personal information sent via email must be encrypted if technically feasible, and if not, then alternative methods to communicating personal information, such as establishing a secure web site, should be considered.[13] Interestingly, few, if any, generally accepted encryption technologies exist for most portable devices (except laptops), and as a result, businesses arguably have an excuse for not encrypting personal information on such devices until technology catches up with the law.[14] Regardless, businesses should consider ways to prevent personal information from being placed at risk on such devices.

CONTRACTS WITH THIRD-PARTY SERVICE PROVIDERS

Another aspect of the Massachusetts Standards that is garnering some attention is the requirement that all service providers must be contractually bound by March 1, 2012, to maintain appropriate security measures to protect personal information consistent with the Massachusetts Standards and any applicable federal regulations. Contracts that were entered into with service providers prior to March 1, 2010, are not required to include such obligations, but for service providers retained after March 1, 2010, businesses must take "reasonable steps" to select service providers that are capable of maintaining such security measures.[15] In the near term, this obligation will likely affect the pricing of third-party services, as service providers are forced to implement additional safeguards, including encryption technologies, to comply with the Massachusetts Standards and future similar regulations. This service provider provision in the Massachusetts Standards is modeled after the service provider provision in the FTC's Safeguards Rule.[16]

ENFORCEMENT

Enforcement of the Massachusetts Standards will be carried out by the Attorney General of Massachusetts. Actions for injunctive relief and civil penalties of not more than $5,000 per violation (plus the reasonable costs of investigation and litigation) may be brought for any violations of the regulation.[17] Enforcement is less likely against businesses that promptly and fully cooperate following a security incident, that can prove the incident was inadvertent, and that can demonstrate compliance with industry best practices for data protection.[18] Factors that the

Attorney General's office will consider in determining whether to take enforcement action include the specifics of the breach, how many Massachusetts residents may be affected, signs of intentional criminal theft, the size of the business and resources available to it, adherence to the business's WISP, and the technical feasibility of implementing measures to prevent the breach.[19]

FUTURE IMPLICATIONS

The Massachusetts Standards will have a widespread effect on how business is conducted by companies throughout the United States and how services are provided by third-party vendors. Even though the regulation only reaches to the personal information of Massachusetts residents, many businesses operating outside of Massachusetts possess such information. And, although it will directly affect the way data is protected, perhaps the most far-reaching effect that this regulation will have is serving as a watershed for similar legislation to be adopted in other states. By joining Nevada in adopting laws that mandate the encryption of personal information, Massachusetts is creating momentum that other states may ride to enact their own encryption laws. States like Michigan, Washington, and New York have considered, or are currently considering, data security legislation with encryption requirements. If the adoption of encryption regulations follows the same course as that of data breach regulations, it will not be long before many more states follow the lead of Nevada and Massachusetts, and the result could have lasting repercussions on the day-to-day operations of virtually every business.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Kevin D. Lyles
+1.614.281.3821
kdlyles@jonesday.com

Mauricio F. Paez
+1.212.326.7889
mfpaez@jonesday.com

Alfred Cheng
+1.214.969.3723
acheng@jonesday.com

ENDNOTES

1 201 Mass. Code Regs. § 17.03(1) (2009).

2 201 Mass. Code Regs. § 17.02 (2009).

3 Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation, "Frequently Asked Question Regarding 201 CMR 17.00," Nov. 3, 2009, *available at* http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf.

4 201 Mass. Code Regs. § 17.03(2) (2009).

5 Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation, "Frequently Asked Question Regarding 201 CMR 17.00," Nov. 3, 2009, *available at* http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf.

6 *Id.*

7 201 Mass. Code Regs. § 17.04 (2009).

8 Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation, "Frequently Asked Question Regarding 201 CMR 17.00," Nov. 3, 2009, *available at* http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf.

9 *Compare* S.B. 227, 2009 Leg., 75th Sess. (Nev. 2009), *with* 201 Mass. Code Regs. § 17.04(5) (2009).

10 *Compare* S.B. 227, 2009 Leg., 75th Sess. (Nev. 2009), *with* 201 Mass. Code Regs. § 17.04(3) (2009).

11 201 Mass. Code Regs. § 17.02 (2009).

12 Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation, "Frequently Asked Question Regarding 201 CMR 17.00," Nov. 3, 2009, *available at* http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf.

13 *Id.*

14 *Id.*

15 201 Mass. Code Regs. § 17.03(2)(f)(2) (2009).

16 Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation, "Frequently Asked Question Regarding 201 CMR 17.00," Nov. 3, 2009, *available at* http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf.

17 Mass. Gen. Laws ch. 93A § 4 (2006).

18 Eric B. Parizo, "MA 201 CMR 17 enforcement less likely with prompt reporting, cooperation," SearchSecurity.com, Jan. 28, 2010, *available at* http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1379916,00.html.

19 *Id.*