

THE INVESTMENT LAWYER™

covering legal and regulatory
issues of asset management

ASPEN PUBLISHERS

Vol. 16, No. 10 • October 2009

REGULATORY MONITOR

Distribution/Marketing
Ballard Spahr LLP
—Denver, CO

—by Paul W. Scott and Ryan M. Howe

Massachusetts Issues Revised Privacy Rules

On August 17, 2009, the Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation released revised Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts (Privacy Rules). Massachusetts' Privacy Rules originally were proposed in 2007, but have been amended several times due to industry opposition to their breadth and scope. The revised rules, however, appear to address the concerns raised by industry participants, such as the Investment Company Institute, and are therefore expected to be adopted. The revised Privacy Rules become effective on March 1, 2010.

The Privacy Rules apply to any person that owns or licenses personal information about a resident of Massachusetts and establish "minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records." [201 CMR 17.01(1).] "Personal information" is defined 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; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." [201 CMR 17.02.] A person "owns or licenses" personal information if they receive, maintain, process or otherwise have access to personal information in connection with the provision of goods or services or in connection with employment.

The most recent revisions to the Privacy Rules generally conform the rules to the SEC's proposed revisions to Reg. S-P. By contrast, prior versions had mandated specific components for information security programs, required contracts with third-party vendors to mandate compliance with the rules, and contained rigid technology requirements for information encryption. These provisions have been replaced with a risk-based approach that allows businesses to develop an information security program that is "appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information." [201 CMR 17.03(1).] The third-party service provider provisions likewise have been modified so that

contracts with third-parties entered into before March 10, 2010, will be deemed to comply with the rules until March 1, 2012, notwithstanding the absence of a provision in the contract that the service provider maintain a comprehensive information security program. In addition, the computer system security requirements of the rule are now required only to the extent the security system is “technically feasible.” [201 CMR 17.04.]

To comply with the rules, an information security program must:

1. Designate an employee to maintain the information security program;
2. Identify reasonably foreseeable internal and external security risks and evaluate and improve current safeguards;
3. Establish policies for employees regarding storage, access, and transportation of personal information off premises;
4. Impose disciplinary measures for violations of the program and prevent former employees from accessing personal information;
5. Oversee third-party service providers by implementing reasonable measures to select service providers that maintain appropriate protections for personal information and requiring contractual agreements to implement security measures to protect personal information;
6. Restrict physical access to personal information and establish procedures to monitor whether the information security program is operating in a manner reasonably calculated to prevent unauthorized access or use of personal information;
7. Review security measures on an annual basis or upon a material change in business procedures; and
8. Implement procedures to document actions taken in connection with a breach and require mandatory post-incident review of events and actions taken.

In addition, an information security program must include the establishment and maintenance of a security system covering computers, including any wireless system, which at a minimum, and to the extent technically feasible, has the following elements:

- Secure user authentication protocols including:
 - Control of user IDs and other identifiers;

- A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
- Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
- Restricting access to active users and active user accounts only; and
- Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- Secure access control measures that restrict access to records and files containing personal information to those who need such information to perform their job duties, and assignment of 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;
- Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly;
- Reasonable monitoring of systems for unauthorized use of or access to personal information;
- Encryption of all personal information stored on laptops or other portable devices;
- For files containing personal information on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information;
- Reasonably up-to-date versions of system security agent software that must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and that is set to receive the most current security updates on a regular basis; and
- Education and training of employees on the proper use of the computer security system

and the importance of personal information security. [See 201 CMR 17.04.]

The revised Privacy Rules provide much needed flexibility by allowing firms to tailor their policies and procedures to the actual risks to

information security that are prevalent in their business. However, the breadth and scope of the Privacy Rules are still substantial and it is important for firms to begin to review their information security programs now to ensure compliance by March 2010.

Reprinted from *The Investment Lawyer* August 2009, Volume 16, Number 10, pages 27-28, with permission from Aspen Publishers, Inc., Wolters Kluwer Law & Business, New York, NY, 1-800-638-8437, www.aspenpublishers.com