The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 23920

November 2, 2009

Massachusetts Adopts Final Privacy Regulations With Compliance Dates of March 1, 2010 and 2012

[23920]

November 2, 2009

TO: BANK, TRUST AND RECORDKEEPER ADVISORY COMMITTEE No. 50-09
BROKER/DEALER ADVISORY COMMITTEE No. 59-09
COMPLIANCE MEMBERS No. 46-09
OPERATIONS MEMBERS No. 23-09
PRIMARY CONTACTS - MEMBER COMPLEX No. 14-09
PRIVACY ISSUES WORKING GROUP No. 14-09
SEC RULES MEMBERS No. 118-09
SMALL FUNDS MEMBERS No. 63-09
TECHNOLOGY COMMITTEE No. 23-09
TRANSFER AGENT ADVISORY COMMITTEE No. 81-09 RE: MASSACHUSETTS ADOPTS FINAL PRIVACY REGULATIONS WITH COMPLIANCE DATES OF MARCH 1, 2010 AND 2012

On Friday, the Massachusetts Office of Consumer Affairs and Business Regulation (the "Agency") published the final version of the Massachusetts Data Privacy Standards (the "Standards"). The adopted version of the Standards is virtually identical to those that were published for comment in August 2009. [1] With the exception of the provision applicable to requiring third party service providers to implement security standards by contract (i.e., Rule 17.03(2)(f)(2)), the compliance date for the Standards is March 1, 2010. The compliance date for Rule 17.03(2)(f)(2) is March 1, 2012. [2] The adopted version is briefly summarized below.

As you may recall, the Institute has long sought to have the Standards revised from the version that was originally published for comment in January 2008 and adopted in

September 2008. We were very pleased with the substantial revisions that were made to them and published for comment in August of this year. Our one remaining concern with them was the fact that the latest version had added a definition of “owns or licenses” that seemed to render moot the provisions in the Standards applicable to third party service providers. [3] Accordingly, the Institute recommended at a hearing in September on the proposed Standards that this definition be deleted. While the definition remains in the Standards, according to the staff of the Agency, the definition (and consequently the Standards) only applies to the person who receives the nonpublic personal information directly from (or on behalf of) a customer who is a Massachusetts resident in connection with the provision of goods or services to such customer. Persons who subsequently receive that information from the original recipient would be third party service providers under the Standards. This interpretation of this definition satisfactorily addresses our concerns.

As with the version of the Standards proposed in August, the final adopted version:

- Revises the definition of encryption to provide more flexibility and requires encryption of data only “to the extent technically feasible;”
- Adds a definition of “service provider,” which limits the scope of the term to a person that is permitted access to personal information and that provides services “directly to a person that is subject to” the Standards;
- Revises Rule 17.03, Duty to Protect and Standards for Protecting Personal Information, to provide greater flexibility by expressly enabling a person to take into account its characteristics, vulnerabilities, sensitivities, and resources when designing an information security program;
- Requires the safeguards in an information security program to be consistent with any requirements imposed by any applicable state or federal law;
- Adds provisions governing the oversight of service providers. Significantly, these provisions only apply to third-party service providers and, consistent with SEC requirements, [4] would require a contract in which the third-party service provider agrees “to implement and maintain such appropriate security measures for personal information.” [5] As noted above, to avoid disrupting existing contracts, the proposal would provide that, so long as a contract was entered into prior to March 1, 2010, it “shall be deemed to be in compliance” with this provision until March 1, 2012, even if it does not include a requirement that the third party service provider maintains appropriate safeguards”; and
- Conditions all requirements in Rule 17.04, Computer System Security Requirements, (including those relating to encryption), on including the requirement in the security system component of the comprehensive information security program only “to the extent technically feasible.”

Importantly for our industry, for the most part, the proposed revisions track the SEC’s proposed revisions to Regulation S-P that would require SEC registrants to have, maintain, and monitor a comprehensive information security program to protect personal information. [6]

A copy of the final version of the Standards is attached. Also attached is a document, "Frequently Asked Questions," ("FAQs") which was published with the proposed Standards in August to explain their contents and scope. Because the final version of the Standards is substantively identical to the version published in August, the information in this document is still valid.

Tamara K. Salmon
Senior Associate Counsel

Attachment

endnotes

[1] See Institute Memorandum No. 23720, dated August 17, 2009.

[2] These dates have not been changed since the August version of the Standards. The Agency believed the compliance date for Rule 17.03(2)(f)(2) was confusing so the language – but not the date – has been revised to be more clear.

[3] This is because the definition includes any person who "receives" nonpublic personal information about a Massachusetts resident.

[4] See, e.g., Section 248.13 of Regulation S-P.

[5] The prior version of the Standards would have required all service providers to be compliant with all provisions in the Standards.

[6] See Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information; Proposed Rule, SEC Release Nos. 34-57427, IC-27178, and IA-2712 (March 4, 2008), 73 Fed. Reg. 13692 (March 13, 2008), which is available at: http://www.sec.gov/rules/proposed/2008/34-57427fr.pdf. Some of the express requirements in the proposed Standards would be consistent with, though not specifically required by the proposed revisions to Reg. S-P (e.g., imposing disciplinary measures for violations of the comprehensive information security program rules; storage of records and data in locked facilities, storage areas or containers). None of these provisions in the Standards raised concerns of note for members.