The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 23720

August 17, 2009

Massachusetts Proposes Revised Privacy Regulations That Address Industry Concerns; September Hearing Scheduled

[23720]

August 17, 2009

TO: BANK, TRUST AND RECORDKEEPER ADVISORY COMMITTEE No. 35-09
BROKER/DEALER ADVISORY COMMITTEE No. 47-09
COMPLIANCE MEMBERS No. 38-09
OPERATIONS MEMBERS No. 17-09
PRIMARY CONTACTS - MEMBER COMPLEX No. 10-09
PRIVACY ISSUES WORKING GROUP No. 9-09
SEC RULES MEMBERS No. 89-09
SMALL FUNDS MEMBERS No. 49-09
TECHNOLOGY COMMITTEE No. 17-09
TRANSFER AGENT ADVISORY COMMITTEE No. 60-09 RE: MASSACHUSETTS PROPOSES REVISED PRIVACY REGULATIONS THAT ADDRESS INDUSTRY CONCERNS; SEPTEMBER HEARING SCHEDULED

As you may know, the Institute has been active and vocal in opposing the provisions of the Massachusetts Data Privacy Standards (the "Standards") since they were originally proposed in 2007. [1] I am very pleased to report that our efforts appear to have paid off. Today, the Agency published for comment the attached proposed revisions to the Standards that are significantly different from, and largely resolve industry concerns with, the current version of the Standards. These concerns, and how they are addressed by the proposal are briefly summarized below.

A hearing on the proposed revisions will be held on September 22nd. The Institute expects to present testimony on them, including our support for their adoption. Persons with any

comments on the proposal should provide them to the undersigned by phone (202-326-5825) or email (tamara@ici.org) no later than Friday, September 11th.

As noted in our most recent letter to the Agency, our concerns with the current version of the Standards are four-fold: (1) their extra-territorial impact; (2) their overly broad scope; (3) their very prescriptive and static nature; and (4) their potential for creating irreconcilable conflicts of law. The proposed revisions to the Standards address these concerns by:

- Limiting their scope to persons who own or license personal information; [2]
- Revising the definition of encryption to provide more flexibility and requiring encryption of data only "to the extent technically feasible;"
- Adding a definition of "service provider" that limits its scope to a person that is permitted access to personal information and that provides services "directly to a person that is subject to" the Standards;
- Revising 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;
- Requiring the safeguards in an information security program to be consistent with any requirements imposed by any applicable state or federal law;
- Adding provisions governing the oversight of service providers. Significantly, these provisions only apply to third-party service providers and, consistent with SEC requirements, [3] would require a contract in which the third-party service provider agrees "to implement and maintain such appropriate security measures for personal information." [4] To avoid disrupting existing contracts, the proposal would provide that, so long as a contract was entered into prior to March 1, 2010, until March 1, 2012, an existing contract with a third-party service provider "shall be deemed to be in compliance" with this provision, "notwithstanding the absence in any such contract of a requirement that the service provider maintain such protective security measures"; and
- Conditioning 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. [5]

Attached are a copy of the proposed revisions, a Notice of the public hearing to be held on them on September 22nd, an Agency press release announcing their publication, and a "Frequently Asked Questions" explaining the proposed revisions and their scope. As noted

in this last document the four “important differences” between the proposal and the existing version of the Standards are:

1. In lieu of an approach that mandates every component of a security program, the proposal adopts a risk-based approach to information security that takes 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.

2. Consistent with (1), the proposal deletes a number of specific provisions required to be included in a business’s written information security program and treats them instead as “guidance.”

3. The encryption requirement has been tailored to be technology neutral and technical feasibility has been applied to all computer security requirements.

4. The third-party vendor requirements have been changed to be consistent with Federal law.

Tamara K. Salmon
Senior Associate Counsel

Attachment

endnotes

[1] Our opposition has included several letters filed with the Massachusetts Office of Consumer Affairs and Business Regulation (the “Agency”), testifying before the Agency and the Legislature on at least three occasions, requesting the introduction of legislation to address our concerns (i.e., Senate Bill 173), and repeated meetings with Massachusetts officials, including senior Agency officials, the Attorney General and her senior staff, and the Lieutenant Governor’s staff. Several members of the Institute joined us in these meetings to impress upon Massachusetts officials the seriousness of our concerns.

[2] The current Standards extend to persons who store or maintain personal information.

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

[4] The current Standards require all service providers to be compliant with all provisions in the Standards.

[5] 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.
