The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 23138

December 19, 2008

Massachusetts Provides Very Limited Guidance on Interpretation of its New Data Security Rules; Compliance Dates Remain Unchanged

[23138]

December 19, 2008

TO: COMPLIANCE MEMBERS No. 67-08
OPERATIONS MEMBERS No. 25-08
PRIMARY CONTACTS - MEMBER COMPLEX No. 21-08
PRIVACY ISSUES WORKING GROUP No. 18-08
SEC RULES MEMBERS No. 144-08
SMALL FUNDS MEMBERS No. 74-08
TECHNOLOGY COMMITTEE No. 34-08
TRANSFER AGENT ADVISORY COMMITTEE No. 71-08 RE: MASSACHUSETTS PROVIDES VERY LIMITED GUIDANCE ON INTERPRETATION OF ITS NEW DATA SECURITY RULES; COMPLIANCE DATES REMAIN UNCHANGED

As you know, in September, Massachusetts announced that it has adopted "Standards for the Protection of Personal Information of Residents of the Commonwealth" (the "Standards"). [1] Since this announcement, the Institute has been working on a variety of fronts – including with the Department that promulgated the rules (the "Department"), the Attorney General's office, and the Legislature – to address our continuing concerns with the overly proscriptive, impractical, extra-territorial, and costly nature of the Standards, as well as with the fact that they exceed the Department's authority under Massachusetts law. As part of these efforts, on November 26th the Institute sent a letter to the Department identifying a variety of provisions within the Standards on which mutual funds need interpretive guidance prior to fully implementing them. By letter dated December 11th, the Department responded to the Institute's letter. Copies of these letters are attached.

While the Department's letter largely failed to respond, or to respond in any meaningful way, to the issues raised in the Institute's letter, it does address one issue relating to certification. In particular, it finds acceptable the form of certification suggested by the Institute to satisfy the Standards' requirement that persons obtain a certification from third-party vendors prior to sharing personal information of Commonwealth residents with such vendors. In particular, the Department has affirmed that the following certification would be acceptable to satisfy the requirement of the rule "provided that, in the case of a corporation, partnership, trust, etc., it contained an averment that the signatory was duly authorized by that entity to make the certification on its behalf." The certification language suggested by the Institute was:

On behalf of ____[name of third-party service provider]_____, I hereby certify that, to the best of our reasonable knowledge and belief, ___[name of third-party service provider]_____ is compliant with the requirements of the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.03 and 17.04 (the "Standards"). In the event this entity becomes aware of any noncompliance with the Standards, we agree to notify all persons to whom we have furnished this certification.

Remaining issues raised in the Institute's November 26th letter and the Department's response are briefly summarized below.

The Institute's letter sought specific guidance from the Department on:

- Whether, if a business maintains an individual's name and social security/account number, there is a duty to determine the state of residence of such person in order to determine whether the individual is a Commonwealth resident;
- Whether personal information merely returned to a person requires a certification from such person prior to being able to return it;
- What is meant by "financial account number;"
- Whether the term "person" includes states other than Massachusetts.

In response, the Department has merely stated that the definition of "personal information" and "person" are taken from the authorizing statute.

The Institute's letter questioned:

- The meaning of "industry standards;"
- The scalability of the Standards' provisions as required by the authorizing statute;
- The meaning of provisions relating to improving safeguards, imposing disciplinary measures, and immediately terminating terminated employees' access;
- The meaning of "third-party service provider" as used in the Standards' provisions requiring amendments to contracts with and certifications from such persons, including dealing with "chains" of third-party service providers as is common in our industry;

- The Standards limiting the use and maintenance of personal information to the "purpose for which it is collected;"
- The application of the Standards to audio recordings (e.g., recorded phone calls) that may contain personal information;
- The interpretation of provisions requiring oversight of the information security program and the documentation of responsive actions taken in connection with breaches, including the retention period for such documents.

In response, the Department has stated:

- Telephone calls containing personal information must be handled in the same manner as other records containing such information;
- Oversight of the program requires both ensuring that it "is being executed in a manner to optimize the security it affords" and analyzing "current, in-house measures in the context," e.g., changes in the company's business or business environment;
- In responding to a breach, a person must maintain documentation that is "detailed enough to accurately record, and to give a reasonable account of, what those responsive actions were;"
- When "evaluating and improving the effectiveness of current safeguards," covered entities "must, at a minimum . . . consider and evaluate the effectiveness of" ongoing employee training, employee compliance with policies and procedures, and means for detecting and preventing security system failures;"
- "A violation of the security program must be a matter with respect to which discipline is warranted. The type of discipline, and how it is meted out, is left to the reasonable determination of the employer;"
- "'Immediately' connotes the absence of undue delay;"
- Portable devices "means devices that are portable;" and
- As regards the provision limiting maintenance of records, according to the Department, "this is a matter that would have to be decided on a case-by-case basis." The Department would expect information provided by a Massachusetts resident in connection with opening a mutual fund account "would be maintained and used for any legitimate purpose connected with that resident's account. . . . If that account were terminated, however, the need to maintain that information would be less obvious, absent state or federal requirements."

As regards the meaning of the provisions in the Standards relating to "third-party service providers," the Department's letter provides the following insight:

. . . a 'third-party service provider' refers to any person or entity that provides a service to the principal to whom the Massachusetts resident delivered his/her personal information. No useful purpose would be served by trying to formulate a definition that will capture every kind of relationship between the recipient to whom a Massachusetts resident delivers his/her personal information and any other person or entity whom that recipient engages to transport, maintain, process, etc., that information; especially so, since third-party service providers are very well known in the mutual fund industry. [2]

The Institute's letter sought clarification of provisions requiring:

- Reasonably secure methods of assigning and selecting passwords;
- That “each person with computer access” be subject to certain requirements;
- “Technically feasible” encryption;
- Electronically transmitted information to be encrypted;
- Security of “data,” as opposed to “personal information;”
- Reasonable monitoring of systems;
- Encryption of “portable devices;”
- Firewalls and patches “on a system connected to the Internet;”
- Use of “reasonably up-to-date” versions of system security software; and
- Training of employees “on the proper use of the computer security system.”

In response, the Department has stated:

- “The method for choosing and assigning passwords must be such as would be adopted by a prudent person . . .;”
- “Each person with computer access” means each person with computer access to personal information;
- “[T]he type/level of encryption is as stated in the definition of that term;”[3]
- It “[does] not believe there is a need to define ‘data’;” and
- “Monitoring,” as used in this provision “relates specifically to ‘unauthorized use of access to personal information.’”

The Institute’s letter also questioned why the “Small Business Guide for Formulating a Comprehensive Information Security Program” that was published by the Department [4] included provisions beyond those required by the rules and was addressed to small businesses, since all provisions of the Standards apply without regard to the size of the business. In response, the Department’s letter noted that the Standards are intended to establish minimum standards and not to preclude or stifle “the implementation of best practices by businesses that are serious about safeguarding the personal information entrusted to them by their customers.”

The Institute will continue to press its concerns with the Standards, as well as with the Department’s response to our letter, with the Department, the Attorney General’s office, and the Legislature. Please note that the compliance dates for the Standards remain unchanged. [5]

Tamara K. Salmon
Senior Associate Counsel

Attachment

endnotes

[1] See Institute Memorandum No. 22901, dated September 23, 2008, for a summary and copy of the Standards.

[2] Because the Institute is at a loss to understand the meaning of this response, in a subsequent letter to the Department, we will, among other issues, seek further guidance

regarding its meaning.

[3] Note that the Standards define “encrypted” to mean “the 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.” See Rule 17.02, “Encrypted.”

[4] See Institute Memorandum No. 23031, dated October 27, 2008 for a summary and copy of the Department’s small business guide.

[5] See Institute Memorandum No. 23066, dated November 14, 2008, relating to extension of the compliance date from January 1, 2009 to January 1, 2010 for provisions relating to certifications and encryption of “portable devices” and May 1, 2009 for all other provisions in the Standards.
