The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 23269

February 23, 2009

Massachusetts Deletes Vendor Certification Requirement From Data Security Standards And Extends Compliance Date To 2010

[23269]

February 23, 2009

TO: BANK, TRUST AND RECORDKEEPER ADVISORY COMMITTEE No. 9-09
BROKER/DEALER ADVISORY COMMITTEE No. 11-09
COMPLIANCE MEMBERS No. 11-09
OPERATIONS MEMBERS No. 6-09
PRIMARY CONTACTS - MEMBER COMPLEX No. 3-09
PRIVACY ISSUES WORKING GROUP No. 2-09
SEC RULES MEMBERS No. 20-09
SMALL FUNDS MEMBERS No. 14-09
TECHNOLOGY COMMITTEE No. 5-09
TRANSFER AGENT ADVISORY COMMITTEE No. 20-09 RE: MASSACHUSETTS DELETES VENDOR CERTIFICATION REQUIREMENT FROM DATA SECURITY STANDARDS AND EXTENDS COMPLIANCE DATE TO 2010

We are very pleased to inform you that, subsequent to the recent hearing on the Massachusetts Data Security Standards (the "Standards"), the Massachusetts Office of Consumer Affairs and Business Regulations (the "Office") has revised the Standards in two very significant ways. [1] First, the revised version eliminates the requirement that persons subject to the Standards obtain a written certification of compliance from each third party service provider with which the person shares personal information about a Massachusetts resident. The revised Standards instead require a person sharing such information to take "all reasonable steps to ensure that such third party service provider is applying to such personal information security measures at least as stringent as those required [under the Standards]." See 201 CMR 17.03(3)(6).

The second significant revision extends the compliance date for all provisions in the Standards until January 1, 2010. See 201 CMR 17.05. Prior to this change, the Office had bifurcated the compliance date, which would have required compliance with some provisions by May 1, 2009 and with others by January 1, 2010. [2]

Since the adoption of the Standards in September 2008, the Institute has been pursuing elimination of the certification requirement and extension of the compliance date, as well as other revisions to the Standards. [3] While the Institute is very pleased with the revisions described above, we will continue to press the additional concerns we have with the Standards, including the fact that they are not consistent with Federal law as required by the Massachusetts law that authorized their adoption.

Tamara K. Salmon
Senior Associate Counsel

Attachment

endnotes

[1] A redlined copy of the revised Standards is attached. For the previous version of the Standards, see Institute Memoranda No. 22901, dated September 23, 2008 (announcing adoption of the Standards) and No. 23066, dated November 14, 2008 (announcing extension and bifurcation of original compliance date).

[2] The Standards were also revised to clarify that the requirement to encrypt data to be transmitted wirelessly only applies to that data containing personal information. See 201 CMR 17.04(3).

[3] See, e.g., Institute Memorandum No. 23138, dated December 19, 2008. At the Office's recent hearing, we submitted both written and oral testimony on these issues. In addition to raising these issues with the Office, we have pursued them with the Office of the Massachusetts Attorney General and raised them in oral and written testimony before the Joint Committee on Consumer Protection and Professional Licensure of the Massachusetts General Assembly.