The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 22901

September 23, 2008

All Funds With Massachussetts Shareholders Or Employees Must Adopt An Information Security Program By January 1st

[22901]

URGENT

September 23, 2008

TO: COMPLIANCE MEMBERS No. 46-08
OPERATIONS MEMBERS No. 16-08
PRIMARY CONTACTS - MEMBER COMPLEX No. 9-08
PRIVACY ISSUES WORKING GROUP No. 13-08
SEC RULES MEMBERS No. 97-08
SMALL FUNDS MEMBERS No. 58-08
TECHNOLOGY COMMITTEE No. 25-08
TRANSFER AGENT ADVISORY COMMITTEE No. 54-08 RE: ALL FUNDS WITH MASSACHUSSETTS SHAREHOLDERS OR EMPLOYEES MUST ADOPT AN INFORMATION SECURITY PROGRAM BY JANUARY 1ST

The Massachusetts Office of Consumer Affairs and Business Regulation has announced that it has adopted “Standards for the Protection of Personal Information of Residents of the Commonwealth” (the “Standards”).* The Standards have an effective date of January 1, 2009. They were promulgated under amendments to Massachusetts laws enacted in 2007 that require the Office to adopt regulations “consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated.” (Emphasis added.) Notwithstanding the consistency requirement in the law, the adopted regulations far exceed requirements currently imposed by the Securities and Exchange Commission on SEC registrants. For example, as noted below, the Standards require persons subject to the rule to obtain written certifications from their third-party service

providers as a precondition to providing the service provider access to personal information.

The Standards, which apply to any person who owns, licenses, stores, or maintains "personal information" about a resident of the Commonwealth of Massachusetts, require such person to (1) have a comprehensive information security program and (2) comply with specified system security requirements. "Personal information" is defined to mean a Massachusetts resident's first 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: (1) Social Security number; (2) driver's license or state identification number; and (3) financial account number or credit or debit card number. The protections required by the Standards for such Massachusetts residents' personal information is discussed in detail below.

Standards for Protection Personal Information

New Rule 17.03 requires every person subject to the Standards to:

. . . develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing . . . personal information [about a resident of the Commonwealth]. Such comprehensive information security program shall be reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records.

The rule expressly requires that the information security program include, but not be limited to, the following:

a. Designating one of more employees to maintain the program;
b. Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks including: (i) ongoing employee training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures;
c. Developing security policies for employees regarding their access and transport of records;
d. Imposing disciplinary measures for violating the program rules;
e. Preventing terminated employees from accessing records containing personal information (e.g., by immediately deactivating their password and user names);
f. Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such information including contractually requiring service providers to maintain safeguards for personal information. Also, prior to permitting third-party service providers access to personal

information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the Standards;

g. Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limiting the time it is retained to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal retention requirements;
h. Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the program provides for the handling of all records as if they all contained personal information;
i. Reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers;
j. Regular monitoring to ensure that the program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and upgrading information safeguards as necessary to limit risks;
k. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and
l. Documenting responsive actions taken in connection with any incident involving a breach of security and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Rule 17.03 additionally provides that, while the program must include each of the above elements, compliance with the rule “shall be evaluated taking into account (i) the size, scope and type of business implementing the program; (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information.”

Computer System Security Requirements

In addition to the above, Rule 17.04 of the Standards require every person subject to the Standards that electronically stores or transmits personal information about a resident of the Commonwealth of Massachusetts to include in its written, comprehensive information security program (required by Rule 17.03) a security system covering its computers, including any wireless system. At a minimum, the system security program shall include each of the following eight elements:

1. Secure user authentication protocols including:
    a. Control of user IDs and other identifiers;
    b. A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
    c. 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;

    d. Restricting access to active users and active user accounts only; and
    e. Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation places on access for the particular system.
2. Security access control measures that:
    a. Restrict access to records and files containing personal information to those who need such information to perform their job duties; and
    b. Assign 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.
3. To the extent technically feasible, encryption of all transmitted files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly.
4. Reasonable monitoring of systems for unauthorized use of or access to personal information.
5. Encryption of all personal information stored on laptops or other portable devices.
6. For files containing personal information on a system that is connected to the Internet, there must be reasonable up-to-date firewall protections and operating system security patches, reasonably designed to maintain the integrity of the personal information.
7. Reasonably up-to-date versions of system security agent software that include malware protection, patches, and virus definitions or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
8. Education and training of employees on the proper use of the computer security system and the importance of personal information security.

Tamara K. Salmon
Senior Associate Counsel
