The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 22482

May 2, 2008

Institute Comment Letter On The SEC's Proposed Amendments To Reg. S-P

[22482]

May 2, 2008

TO: CLOSED-END INVESTMENT COMPANY MEMBERS No. 15-08
COMPLIANCE MEMBERS No. 19-08
INVESTMENT ADVISER MEMBERS No. 8-08
OPERATIONS MEMBERS No. 5-08
PRIVACY ISSUES WORKING GROUP No. 3-08
SEC RULES MEMBERS No. 39-08
SMALL FUNDS MEMBERS No. 28-08
TECHNOLOGY COMMITTEE No. 12-08
TRANSFER AGENT ADVISORY COMMITTEE No. 24-08
UNIT INVESTMENT TRUST MEMBERS No. 8-08 RE: INSTITUTE COMMENT LETTER ON THE SEC'S PROPOSED AMENDMENTS TO REG. S-P

As we previously informed you, last month the Securities and Exchange Commission proposed for comment extensive amendments to Rule 248.30 in Regulation S-P that would require each SEC registrant to have a detailed, rigorous, and robust information security program. [1] The program must comply with certain conditions set forth in the rule relating to the program's objectives, safeguards, testing requirements, notice, and recordkeeping requirements, among others. Based upon comments received from members, the Institute has filed with the Commission the attached comment letter, which is briefly summarized below.

The letter expresses the Institute's support for the Commission's adoption of a more robust data security rule and for including transfer agents within the rule's scope. It recommends, however, several revisions to the Commission's proposal to facilitate compliance and better align its requirements with its intent and the provisions in the Gramm-Leach-Bliley Act (the

"GLB Act") that are the basis for the Commission's rulemaking. In particular, the letter recommends that the Commission:

- Permit registrants to assign responsibility for the program's implementation to either a position that is charged with being the information security program coordinator or to a named individual;
- Clarify that, for registered investment companies, the rule's testing requirements are to be addressed under the testing requirements of Rule 38a-1, the Mutual Fund Compliance Program rule;
- Only require breach notices in the event that the breach will result in a significant risk of substantial harm or inconvenience to a customer;
- Clarify and conform the breach notice standards used for individuals to those applicable to informing the Commission of a breach on Form SP-30;
- Streamline the contents of Form SP-30 and address issues relating to its filing, such as access and immunity from liability for statements on the Form;
- In the event a breach involves more than one entity (e.g., if the breach occurs at a service provider maintaining the fund's information), only require one entity to provide notice to individuals and the SEC, and enable the parties to determine the entity responsible for such notice;
- Conform the data subject to the rule to that subject to the Commission's rulemaking authority under the GLB Act by deleting references to information relating to employees, investors, and securityholders;
- Provide a sufficient compliance period of not less than 24 months; and
- Require the Commission and each registered self-regulatory organization ("SRO") to have an information security program similar to that proposed in Reg. S-P.

Each of these recommendations is discussed in detail in the letter.

With respect to the last bullet, the letter cites a November 2007 GAO Report and a March 2008 report by the SEC's Inspector General that document lax information security practices at the Commission. The letter notes that, when a registrant's data is provided to the SEC or an SRO pursuant to an inspection or investigation, it should have the same level of protection as it does when maintained by the registrant. Moreover, to the extent there is a breach of such information when held by the SEC or the SRO, the registrant should be notified about the breach so it can take appropriate action. Such notice is not currently required by law.

Tamara K. Salmon
Senior Associate Counsel

Attachment

endnotes

[1] See Institute Memorandum No. 22305, dated March 7, 2008 summarizing *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information*, SEC Release Nos. 34-57427, IC-28178, and IA-2712 (March 4, 2008) (the "Release"), available at http://www.sec.gov/rules/proposed/2008/34-57427.pdf. The proposed requirements are patterned after similar provisions adopted by other federal regulators of financial institutions in 2001 to implement the Gramm-Leach-Bliley Act.
