The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 22710

July 17, 2008

Funds With Transaction Accounts Must Obtain Board Approval Of An Identity Theft Prevention Program By November 1st

[22710]

URGENT

July 17, 2008

TO: COMPLIANCE MEMBERS No. 27-08
OPERATIONS MEMBERS No. 9-08
PRIMARY CONTACTS - MEMBER COMPLEX No. 4-08
PRIVACY ISSUES WORKING GROUP No. 5-08
SEC RULES MEMBERS No. 62-08
SMALL FUNDS MEMBERS No. 41-08
TECHNOLOGY COMMITTEE No. 16-08
TRANSFER AGENT ADVISORY COMMITTEE No. 33-08 RE: FUNDS WITH TRANSACTION ACCOUNTS MUST OBTAIN BOARD APPROVAL OF AN IDENTITY THEFT PREVENTION PROGRAM BY NOVEMBER 1ST

EFFECTIVE NOVEMBER 1, 2008, investment companies that are "financial institutions" must have established and obtained board approval of an Identity Theft Prevention Program ("Program") as discussed below. [1] For purposes of this requirement, the term "financial institution" means any person or institution that "directly or indirectly holds a transaction account belonging to a consumer." (See 15 USC §1681a(t)). A "transaction account" is an account:

> . . . on which the . . . account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or similar items for the purpose of making payments or transfers to

third persons or others.

In other words, to the extent an investment company's shareholders are permitted to make withdrawals (redemptions) payable to third persons by check, transferable or negotiable instruments, or similar items (e.g., debit cards), the investment company may be a "financial institution" for purposes of these requirements.

Establishment of a Program

The rule requires financial institutions to establish a Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" [2] or an existing covered account. The Program must include reasonable policies and procedures to:

- Identify relevant "Red Flags"[3] for the covered accounts that the financial institution offers or maintains and incorporate them into the financial institution's Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution from identity theft.

The Program must be applied to the financial institution's covered accounts, and be appropriate to the size and complexity of the financial institution and the nature and scope of its activities. The rule requires a financial institution to consider specified guidelines and include in its Program those guidelines that are appropriate. (See Guidelines, below.)

Administration of the Program

The rule requires that the financial institution:

- Obtain approval of the initial written Program from either the institution's board of directors or an appropriate committee of the board of directors;
- Involve the board of directors, an appropriate committee thereof, or a designated employee (at the level of senior management) in the oversight, development, implementation, and administration of the Program;
- Train staff, as necessary, to effectively implement the Program; and
- Exercise appropriate and effective oversight of service provider arrangements.

Guidelines

Appendix A to the rule sets forth detailed Guidelines a financial institution must

consider in establishing and administering its Program. These Guidelines are divided into three sections:

- Identifying Relevant Red Flags – which discusses Risk Factors; Sources of Red Flags; and Categories of Red Flags;
- Detecting Red Flags – which discusses the need for financial institutions to verify the identity of and authenticate covered account holders, monitor transactions, and verify change of address requests;
- Preventing and Mitigating Identity Theft – which discusses how a financial institution might respond to suspected identity theft, such as contacting the customer and changing passwords; and
- Updating the Program – which discusses the need to update the Program periodically to reflect changes in experiences with identity theft or its detection, prevention, and mitigation and changes in the financial institution's business.

Members with questions regarding the rule or Program requirements should contact the undersigned by phone (202-326-5825) or email (tamara@ici.org).

Tamara K. Salmon
Senior Associate Counsel

endnotes

[1] 2003 amendments to the Fair Credit Reporting Act required the Federal banking regulators, the National Credit Union Administration, and the Federal Trade Commission (FTC) (but not the Securities and Exchange Commission) to prescribe regulations requiring each "financial institution" and each "creditor" to establish reasonable policies and procedures to implement guidelines to detect and prevent identity theft involving account holders or customers of such institutions. As discussed in this memo and as confirmed by the SEC staff, the rule adopted by the FTC appears to apply to investment companies that hold transaction accounts. See Identify Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, Final Rule, 72 Fed. Reg. 63718 (November 9, 2007), which is available at: http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf (the "rule"). The FTC's rule (Rule 681.2) within this joint agency rulemaking can be found on pp. 63772-63774.

[2] "Covered account" is defined in the rule to mean: (1) an account that the financial institution offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments and (2) any other account that the financial institution offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution from identity theft, including financial, operational, compliance, reputation, or litigation risks.

[3] “Red Flag” is defined in the rule to mean “a pattern, practice, or specific activity that indicates the possible existence of identify theft.” Because of the rule’s focus on Red Flags, it is often referred to as the “Red Flag Rule.”
