New FTC Rule Affecting Some Investment Companies Requires Board Approval of Identity Theft Prevention Programs by Nov. 1

DrinkerBiddle

A rule recently adopted by the Federal Trade Commission will affect investment companies that offer transaction accounts, requiring that they have board approval of an identity theft prevention program by Nov. 1, 2008. The rule, issued as part of a joint agency rulemaking, implements part of the Fair and Accurate Credit Transactions Act of 2003, which amended the Fair Credit Reporting Act. The rule impacts, for example, money market funds or any other investment company that permits payment or transfers to third parties such as through check writing or wire transfers.

Companies That Must Comply

Specifically, the rule applies to all "financial institutions," which are entities (including investment companies) that directly or indirectly hold "a transaction account belonging to a consumer." A "transaction account" is a deposit or account from which the depositor or account holder can make withdrawals to make payments or transfers to third persons or others. The withdrawals may be by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers or other similar items, such as debit cards. If an investment company's shareholders can make these types of withdrawals, it would be considered a "financial institution." It should be emphasized that the rule affects only those investment companies that offer transaction accounts to investors, *i.e.*, that are financial institutions.

These financial institutions must develop and implement a written identity theft prevention program (Program) designed to detect, prevent and mitigate identity theft in connection with its covered accounts. (Covered accounts are those that are maintained or offered primarily for personal purposes, and permit multiple payments or transactions, such as a credit card account, mortgage or car loan, or checking, savings or margin accounts.)

Identity Theft Program Requirements

The Program, which may include existing policies and procedures, must incorporate four requirements:

1. **Identify relevant "red flags" (patterns, practices or activities that indicate the possibility of identity theft) for covered accounts and incorporate those red flags into the Program.**

   Consider the following factors: the types of covered accounts offered/maintained, the methods provided to open them, the methods used to access the accounts and the financial institution's previous experiences with identity theft.

2. **Detect red flags.**

   Obtain identifying information about and verify the identity of people opening covered accounts, authenticate customers, monitor transactions and verify the validity of change of address requests.

3. **Respond appropriately to any detected red flags.**

   Provide appropriate responses to the red flags detected that are commensurate with the degree of risk posed. Consider aggravating factors that may heighten the risk of identity theft, such as a prior data security incident. Responses to red flags may include monitoring a covered account for evidence of identity theft, contacting the customer, changing passwords or security codes, reopening a covered account with a new account

number, notifying law enforcement, or determining that no response is warranted.

4. **Ensure that the Program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the financial institution with respect to identity risk.**

   When determining whether it is time to update the Program, consider the financial institution's experiences with identity theft, changes in the types of accounts offered/maintained, and changes in the institution's business arrangements (*i.e.*, any mergers, acquisitions or joint ventures).

Identity Theft Program Administration

To administer the Program, a financial institution must:

- **Obtain approval of the initial written Program from either the board of directors or its appropriate committee by Nov. 1, 2008.**

  Oversight of the Program should include assigning specific responsibility for the Program's implementation, reviewing reports prepared by staff regarding compliance and approving material changes to the Program as necessary to address changing identity theft risks.

- **Involve the board, its appropriate committee or a designated senior-management employee in the development, implementation, oversight and administration of the Program.**

  Oversight of the Program should include assigning specific responsibility for the Program's implementation, reviewing reports prepared by staff regarding compliance and approving material changes to the Program as necessary to address changing identity theft risks.

- **Train staff to implement the Program.**

  Staff should report to the board, its appropriate committee or a designated senior-level management employee at least annually on compliance with the rule. The report should address and evaluate material matters such as the effectiveness of the Program, significant incidents involving identity theft and management's response, service-provider arrangements and recommendations for material changes.

- **Exercise oversight of service-provider arrangements.**

  A financial institution should take steps to ensure that the activity of the service provider is conducted in accordance with the institution's policies and procedures designed to detect, prevent and mitigate the risk of financial theft.

The FTC rule is available at: http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf. (See Rule 681.2, the FTC's rule within this joint agency rulemaking and the guidelines that follow in Appendix A, on pp. 63722-63774.)

For more information about the matters discussed in this Alert, please contact your regular Drinker Biddle lawyer or any member of our Investment Management Group.

Investment Management Practice Group

Partners and Counsel

Gary D. Ammon
(215) 988-2981
Gary.Ammon@dbr.com

Jeffrey Blumberg
(312) 569-1106
Jeff.Blumberg@dbr.com

Stephen T. Burdumy
(215) 988-2880
Stephen.Burdumy@dbr.com

Glenn E. Ferencz
(312) 569-1246
Glenn.Ferencz@dbr.com

Stephen D.D. Hamilton
(215) 988-1990
Stephen.Hamilton@dbr.com

Veena K. Jain
(312) 569-1167
Veena.Jain@dbr.com

Morgan R. Jones
(215) 988-2792
Morgan.Jones@dbr.com

Michelle M. Lombardo
(215) 988-2867
Michelle.Lombardo@dbr.com

Michael P. Malloy
(215) 988-2978
Michael.Malloy@dbr.com

David M. Matteson
(312) 569-1145
David.Matteson@dbr.com

Diana E. McCarthy
(215) 988-1146
Diana.McCarthy@dbr.com

Mary Jo Reilly
(215) 988-1137
MaryJo.Reilly@dbr.com

Audrey C. Talley
(215) 988-2719
Audrey.Talley@dbr.com

DrinkerBiddle

LAW OFFICES | CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY
NEW YORK | PENNSYLVANIA | WASHINGTON DC | WISCONSIN