DechertOnPoint

August 2008 / Issue 20

A legal update from Dechert's Financial Services Group

Certain Funds Must Implement Identity Theft Prevention Programs by November 1, 2008

Effective November 1, 2008, Federal Trade Commission ("FTC") rules will require certain investment companies, including funds with check-writing privileges, to develop, implement, and obtain board approval of a written identity theft prevention program. As discussed below, an investment company must comply with the FTC rules, commonly known as the "Red Flag Rules," if it directly or indirectly holds a "transaction account" belonging to a consumer. Procedures implemented in accordance with the Red Flag Rules must identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft ("Red Flags").

Background

The President signed the Fair and Accurate Credit Transaction Act of 2003 ("FACT Act") into law on December 4, 2003.[1] The FACT Act directs certain federal agencies to issue regulations and guidelines regarding the detection, prevention, and mitigation of identity theft. On July 18, 2006, the FTC, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration (collectively, the "Agencies") jointly proposed the Red Flag Rules to implement the FACT Act.[2] The Agencies issued the final Red Flag Rules on November 9, 2007, requiring compliance by November 1, 2008.[3]

Relevance to Investment Companies

The Red Flag Rules apply to "financial institutions" with "covered accounts."[4] The staff of the Securities and Exchange Commission recently confirmed that investment companies must implement an identity theft prevention program in accordance with the Red Flag Rules if it meets the Agencies' definitions of these terms.[5]

---

1 Fair and Accurate Credit Transaction Act of 2003, Pub. L. No. 108-159 (2003).

2 Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Proposed Rule, 71 Fed. Reg. 40786 (Jul. 18, 2006).

3 Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule, 72 Fed. Reg. 63718 (Nov. 9, 2007).

4 The Red Flag Rules also apply to "creditors" with covered accounts. *Id.* at 63719.

5 Memorandum from the Investment Company Institute to Compliance Members (July 17, 2008), *available at* http://members.ici.org/getMemoPDF.do?file=22710.ICINET.DOC.pdf.

An investment company is considered a "financial institution" if it directly or indirectly holds a "transaction account" belonging to a consumer.[6] A transaction account is defined as "a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others."[7] Examples of transaction accounts include "demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts."[8] Thus, an investment company that offers shareholders the ability to redeem shares to third-persons by checks or debit cards, for example, is a "financial institution" under the Red Flag Rules.

The Red Flag Rules define a "covered account" as "an account that a financial institution . . . maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions" or "any other account that the financial institution . . . maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution . . . from identity theft . . ."[9] Examples of covered accounts include checking accounts, savings accounts, and margin accounts.

Red Flag Categories

The Agencies identified five categories of Red Flags when jointly issuing the Red Flag Rules:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- The presentation of suspicious documents;
- The presentation of suspicious personal identifying information, such as a suspicious address change;
- The unusual use of, or other suspicious activity related to, a covered account; and
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by a financial institution.

The Agencies also provided twenty-six examples of Red Flags to illustrate the scope of activity that financial institutions' identity theft prevention procedures must address.[10]

Compliance with the Red Flag Rules

A financial institution subject to the Red Flag Rules must develop a written program designed to identify, detect and respond to the Red Flags relevant to the financial institution's "covered accounts," and obtain board-approval of such program by November 1, 2008. The Agencies' guidelines for fulfilling these requirements are summarized below:

- *Identification*. When identifying the Red Flags relevant to its covered accounts, a financial institution should consider (i) the types of covered accounts it offers or maintains; (ii) the methods it provides to open its covered accounts; (iii) the methods it provides to access its covered accounts; and (iv) its previous experiences with identity theft.[11]
- *Detection*. A financial institution's procedures should address the detection of Red Flags in connection with both the opening of covered accounts and the maintenance of existing accounts. In connection with the opening of accounts, examples of detection procedures include procedures for (i) obtaining information about the person opening an account; and (ii) verifying the identity of the person opening an account. In connection with the maintenance of existing accounts, examples of detection procedures include procedures for (i) authenticating customers; (ii) monitoring transactions; and (iii) verifying the validity of change of address requests.[12]
- *Response*. A financial institution's procedures should provide for appropriate responses to the Red Flags the institution detects. Such responses should be commensurate with the degree of risk

6 *Id.* at 63722 (referencing 15 U.S.C. § 1681a(t) (2006)).

7 15 U.S.C. § 1681a(t) (2006) (referencing 12 U.S.C. § 461(b)(1)(C) (2006).

8 12 U.S.C. § 461(b)(1)(C) (2006).

9 Red Flag Rules, *supra* note 3, at 63721.

10 *Id.* at 63773-774.

11 *Id.* at 63773.

12 *Id.*

posed and may include (i) monitoring a covered account; (ii) contacting a customer; (iii) changing any passwords or other security devices that permit access to a covered account; (iv) reopening a covered account with a new account number; (v) not opening a new covered account; (vi) closing an existing covered account; (vii) not attempting to collect on a covered account or not selling a covered account to a debt collector; (viii) notifying law enforcement; or (ix) determining that no response is warranted.[13]

- *Administration*. A financial institution's procedures must be managed by the institution's board of directors, an appropriate committee of the board of directors, or a designated senior management employee. Such management must include (i) assigning specific responsibility for the financial institution's implementation of its procedures; (ii) reviewing compliance reports prepared by the institution's staff; and (iii) approving material changes to the institution's procedures as necessary to address changing identity theft risks.[14]

- *Updates*. Financial institutions should periodically update their procedures based on factors such as (i) the experiences of the institution with identity theft; (ii) changes in methods of identity theft; (iii) changes in methods to identify, detect, prevent and mitigate identity theft; (iv) changes in the types of accounts that the financial institution offers or maintains; and (v) changes in the business arrangements of the financial institution, including mergers, acquisitions, alliances and service provider arrangements.[15]

Conclusion

Dechert LLP will continue to monitor developments in this area.

■ ■ ■

This update was authored by David Harris (+1 202 261 3385; david.harris@dechert.com), Anthony H. Zacharski (+1 860 524 3937; anthony.zacharski@dechert.com), Alan Rosenblat (+1 202 261 3332; alan.rosenblat@dechert.com), and Thomas C. Bogle (+1 202 261 3360; thomas.bogle@dechert.com). Research assistance provided by John P. Foley, Summer Associate.

13 *Id.*

14 *Id.*

15 *Id.*

Practice group contacts

For more information, please contact the authors, one of the attorneys listed, or any Dechert attorney with whom you regularly work. Visit us at www.dechert.com/financialservices.

Margaret A. Bancroft
New York
+1 212 698 3590
margaret.bancroft@dechert.com

Sander M. Bieber
Washington, D.C.
+1 202 261 3308
sander.bieber@dechert.com

Stephen H. Bier
New York
+1 212 698 3889
stephen.bier@dechert.com

Daphne T. Chisolm
Charlotte
+1 704 339 3153
daphne.chisolm@dechert.com

Christopher D. Christian
Boston
+1 617 728 7173
christopher.christian@dechert.com

Elliott R. Curzon
Washington, D.C.
+1 202 261 3341
elliott.curzon@dechert.com

Douglas P. Dick
Washington, D.C.
+1 202 261 3305
douglas.dick@dechert.com

Ruth S. Epstein
Washington, D.C.
+1 202 261 3322
ruth.epstein@dechert.com

Susan C. Ervin
Washington, D.C.
+1 202 261 3325
susan.ervin@dechert.com

Joseph R. Fleming
Boston
+1 617 728 7161
joseph.fleming@dechert.com

Brendan C. Fox
Washington, D.C.
+1 202 261 3381
brendan.fox@dechert.com

Wendy Robbins Fox
Washington, D.C.
+1 202 261 3390
wendy.fox@dechert.com

David M. Geffen
Boston
+1 617 728 7112
david.geffen@dechert.com

David J. Harris
Washington, D.C.
+1 202 261 3385
david.harris@dechert.com

Robert W. Helm
Washington, D.C.
+1 202 261 3356
robert.helm@dechert.com

Jane A. Kanter
Washington, D.C.
+1 202 261 3302
jane.kanter@dechert.com

Geoffrey R.T. Kenyon
Boston
+1 617 728 7126
geoffrey.kenyon@dechert.com

George J. Mazin
New York
+1 212 698 3570
george.mazin@dechert.com

Jack W. Murphy
Washington, D.C.
+1 202 261 3303
jack.murphy@dechert.com

John V. O'Hanlon
Boston
+1 617 728 7111
john.ohanlon@dechert.com

Jeffrey S. Puretz
Washington, D.C.
+1 202 261 3358
jeffrey.puretz@dechert.com

Jon S. Rand
New York
+1 212 698 3634
jon.rand@dechert.com

Robert A. Robertson
Newport Beach
+1 949 442 6037
robert.robertson@dechert.com

Keith T. Robinson
Hong Kong
+1 852 3518 4705
keith.robinson@dechert.com

Alan Rosenblat
Washington, D.C.
+1 202 261 3332
alan.rosenblat@dechert.com

Kevin P. Scanlan
New York
+1 212 649 8716
kevin.scanlan@dechert.com

Frederick H. Sherley
Charlotte
+1 704 339 3100
frederick.sherley@dechert.com

Patrick W. D. Turley
Washington, D.C.
+1 202 261 3364
patrick.turley@dechert.com

Brian S. Vargo
Philadelphia
+1 215 994 2880
brian.vargo@dechert.com

David A. Vaughan
Washington, D.C.
+1 202 261 3355
david.vaughan@dechert.com

Anthony H. Zacharski
Hartford
+1 860 524 3937
anthony.zacharski@dechert.com

Dechert LLP

www.dechert.com

U.S. Austin • Boston • Charlotte • Hartford • Newport Beach • New York • Philadelphia Princeton • San Francisco • Silicon Valley • Washington, D.C. • **EUROPE** Brussels London • Luxembourg • Munich • Paris • **ASIA** Hong Kong