Client Alert

pillsbury

Executive Compensation & Benefits

April 22, 2009

# Approaching Enforcement Date for the "Red Flags Rule" Raises Questions for Some 401(k) Plan Sponsors

by Susan P. Serota and Bradley A. Benedict[1]

*Plan sponsors that are considered "financial institutions" or "creditors" (as defined below) may be subject to the Red Flags Rule on and after May 1, 2009, with respect to employee benefit plans that offer plan loans or feature individual accounts. The Red Flags Rule requires certain entities to establish a written program to prevent, detect, and mitigate identity theft associated with certain types of accounts. A 401(k) plan or other benefit plan could fall within the scope of the regulations.*

The following Q&As explain the Red Flags Rule, provide guidance on determining whether the Rule applies to an entity, and outlines the Rule's requirements.

## What Is the Red Flags Rule?

The Red Flags Rule was promulgated by the Federal Trade Commission ("FTC") and other bank regulatory agencies under the Fair and Accurate Credit Transactions Act of 2003 (the "Act").[2] Its purpose is to combat identity theft arising from the establishment and operation of consumer accounts and certain other types of accounts. The Rule affects "financial institutions" and "creditors," as defined in the Act (together, "Covered Entities"). But only those Covered Entities offering or maintaining "Covered Accounts" (as defined below) must adopt a written identity theft prevention program.

[1] Awaiting bar admission; supervised by members of the New York Bar.

[2] Pub. L. No. 108-159 (Dec. 4, 2003), § 114 (codified in 15 U.S.C. 1681m, amending Section 615 of the Fair Credit and Reporting Act); see also 72 Fed. Reg. 63718-75 (Nov. 9, 2007).

## What is a "financial institution" and "creditor" under the Red Flags Rule?

The Rule applies to a wide range of entities. For purposes of the Rule, a "financial institution" means a bank, credit union, or savings and loan association and "any other person that, directly or indirectly, holds a transaction account … belonging to a consumer." A "creditor" under the Rule includes any person that regularly extends, renews or continues credit or regularly arranges for the extension, renewal or continuation of credit, among others.

## What is a Covered Account under the Red Flags Rule?

There are two categories of Covered Accounts. The first category includes consumer-type accounts, intended primarily for personal, family, or household purposes, that permit the account holder to make multiple payments or transactions.

The second category includes any other account "for which there is a reasonably foreseeable risk to customers[3] or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks." Unlike the first category, these arrangements are Covered Accounts only if they involve a reasonably foreseeable risk of identity theft. Covered Entities must periodically evaluate whether any of their accounts fall within this second category due to changes in practices or in the nature of the identity theft risks involved.

## What are the implications for sponsors of employee benefit plans?

An entity is subject to the Red Flags Rule if (1) it is a Covered Entity and (2) it maintains either category of Covered Account. Two areas of concern with respect to employee benefit plans are plans that allow participants to borrow against their account balance and plans featuring individual accounts sponsored by employers that are Covered Entities irrespective of their benefits plans.

### Plan Loans

Arguably, the sponsor of a plan that includes a loan feature would be a "creditor" under the Red Flags Rule because the plan permits the extension of credit to participants. The FTC, however, has informally indicated that benefit plan sponsors would not be considered creditors based solely on the existence of a plan loan feature. The agency noted that whether an entity "regularly" extends credit (or arranges for the extension of credit) is a facts-and-circumstances determination. The FTC suggested that isolated or incidental credit extensions would likely be insufficient to confer creditor status and, further, that the Truth in Lending Act's definition of "regularly" (generally requiring a frequency of 25 instances per year) does not apply to the Red Flags Rule. Unless further guidance is issued, plan sponsors should consider the nature and frequency of their plan loans to determine whether they may be deemed a creditor subject to the Rule. If a determination is made that the plan sponsor is a creditor, and therefore a Covered Entity, it must then determine whether the plan has Covered Accounts.

### Covered Entities that Sponsor Individual Account Plans

If a Covered Entity sponsors a plan that permits participants to manage an individual plan account (like many 401(k) plans), the sponsor may be considered to maintain Covered Accounts. Although such plan accounts do not appear to fall within the first category of Covered Account, they might fall within the scope

[3] "Customer" for this purpose means any person who has a covered account with a financial institution or creditor. The term is not intended to limit this aspect of the rule to consumer-type arrangements.

of the second—i.e., any account that poses a reasonably foreseeable risk from identity theft. This assessment is based on the administration of the relevant accounts, including how they are opened and accessed. Plan accounts that can be managed remotely (e.g., by Internet or telephone) might pose greater risks, for example. Covered Entities must also consider actual incidents of identity theft relevant to similarly administered accounts.

Plan accounts are often administered by third-party service providers, which may also be subject to the Red Flags Rule. Nevertheless, if a plan sponsor that is a Covered Entity determines that its plan has Covered Accounts, it will need to put in place its own identity theft prevention program. Such a program, however, might focus primarily on oversight of the service provider and the service provider's program.

## What does compliance with Red Flags Rule entail?

The initial requirement for any financial institution or creditor is to determine whether it has Covered Accounts. If not, no further action is necessary, other than to reconsider from time to time whether subsequent circumstances trigger the Red Flags Rule. If the answer is yes, the Covered Entity must institute a written program designed to prevent, detect, and mitigate identity theft in connection with the opening of new accounts and the operation of existing ones.

Due to the wide variety of entities and circumstances that fall within the scope of the Rule, the regulations are designed to be extremely flexible. However, the following requirements apply to any financial institution or creditor having Covered Accounts:

- There must be a written program to (1) identify relevant red flags for the applicable Covered Accounts; (2) detect those red flags in managing the Accounts; (3) respond to any red flags that arise to prevent and/or mitigate identity theft; and (4) periodically update the program to reflect operational changes and/or developments in identity theft prevention practices;

- The guidelines provided in Appendix J of the regulations must be considered and incorporated into the program if appropriate;

- The Covered Entity's board of directors (or, if there is no board, a senior-management level employee) must approve the written program;

- The board or its designee (either a board committee or designated senior-level employee) must be involved in the administration and implementation of the program, including the training of staff, as necessary, to implement it effectively; and

- The program must provide for appropriate and effective oversight of service provider arrangements, if any.

Organizations are expected to customize their programs as appropriate for their situation. Where the risk of identity theft is small, a "streamlined" program that incorporates only a few red flags may be sufficient. In designing a program, plan sponsors should consider factors such as the nature, size, and scope of the plan; the procedures for managing individual accounts; and the particular identity theft-related risks associated with its practices. Where access to accounts is restricted and the number of individuals eligible to open accounts is limited, common tools to ensure identity verification and authentication can be incorporated into the program. For example, comparing identifying documents or information to ensure that only appropriate individuals are opening plan accounts and requiring the use of personal identification

numbers (PINs) and passwords for account access are among the measures suggested to detect red flags.

## How is the Red Flags Rule enforced?

There are no criminal penalties for failing to comply with the Red Flags Rule, but violations may subject Covered Entities to civil monetary penalties of up to $3500 per violation under the Fair Credit and Reporting Act. There is no private right of action for violations, but noncompliance could potentially subject a Covered Entity to liability in lawsuits brought under state consumer protection laws or negligence actions.

Although the final regulations adopting the Red Flags Rule became effective on November 1, 2008, the FTC suspended enforcement until May 1, 2009. Every entity potentially within the scope of the rule should determine whether their activities include the management of Covered Accounts to ascertain whether further action is necessary.

**Live Links**

Information on the Fair Credit Reporting Act, including various links on "Red Flags Rule Guidance"
http://www.ftc.gov/os/statutes/fcrajump.shtm

"Fighting Fraud with the Red Flags Rule: A How-To Guide for Business"
http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf

"Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy" (linking to Federal Register, Vol. 72, No. 217 (Nov. 9, 2007)) http://www.ftc.gov/opa/2007/10/redflag.shtm

---

For further information, please contact:

## New York

Susan P. Serota (bio)
+1.212.858.1125
susan.serota@pillsburylaw.com

Peter J. Hunt (bio)
+1.212.858.1139
peter.hunt@pillsburylaw.com

Scott E. Landau (bio)
+1.212.858.1598
scott.landau@pillsburylaw.com

John J. Battaglia (bio)
+1.212.858.1738
john.battaglia@pillsburylaw.com

Mark C. Jones (bio)
+1.212.858.1430
mark.jones@pillsburylaw.com

Bradley A. Benedict *
+1. 212.858.1523
bradley.benedict@pillsburylaw.com

Kathleen D. Bardunias
+1.212.858.1905
kathleen.bardunias@pillsburylaw.com

## Washington, DC / Northern Virginia

Howard L. Clemons (bio)
+1.703.770.7997
howard.clemons@pillsburylaw.com

Keith R. Kost (bio)
+1.703.770.7799
keith.kost@pillsburylaw.com

Clare Stoudt (bio)
+1.202.663.9338
clare.stoudt@pillsburylaw.com

## San Diego – North County

Jan H. Webster (bio)
+1.858.509.4012
jan.webster@pillsburylaw.com

Daniel N. Riesenberg (bio)
+1.858.847.4130
daniel.riesenberg@pillsburylaw.com

Kenneth E. Bonus (bio)
+1.858.847.4206
kenneth.bonus@pillsburylaw.com

## San Francisco

Christine L. Richardson (bio)
+1.415.983.1826
crichardson@pillsburylaw.com

## Silicon Valley

Cindy V. Schlaefer (bio)
+1.650.233.4023
cindy.schlaefer@pillsburylaw.com

Grace Chen (bio)
+1.650.233.4873
grace.chen@pillsburylaw.com

* Awaiting bar admission, supervised by members of the New York Bar