Client Alert

pillsbury

Privacy & Data Protection

Global Sourcing

Life Sciences & Health Care

July 30, 2009

FTC Again Extends Enforcement of Identity Theft Red Flag Rule, to Nov. 1, 2009

by Catherine D. Meyer, John L. Nicholson and Meighan E. O'Reardon

On January 1, 2008, six federal agencies[1] issued final Rules on Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions (FACT) Act of 2003.[2] The Rules implement § 114 and § 315 of the FACT Act, which specifically call for "establishment of procedures for the identification of possible instances of identity theft" and "reconciling addresses."[3] Guidelines and supplemental information were released to assist entities who were originally required to comply by November 1, 2008. Companies under FTC jurisdiction have been granted two extensions to date and enforcement was set to begin on August 1, 2009. However, the deadline has been extended again. FTC-regulated companies now have until November 1, 2009 to comply.

Many companies and industry groups have struggled with the question of whether they are required to comply with the FTC's Red Flag Rule (the "Rule"). The FTC extended the original enforcement deadline from November 1, 2008, to May 1, 2009, to provide additional time for companies under its jurisdiction to achieve compliance. On April 30, 2009, the FTC further extended the enforcement deadline to August 1, 2009. Now, in a press released issued by the FTC on July 29, 2009, companies under the FTC's jurisdiction have an additional three months to comply.[4] This most recent extension pushes the deadline to November 1, 2009.

[1] The Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Federal Trade Commission and the Department of Treasury's Office of the Comptroller of the Currency and Office of Thrift Supervision.

[2] 72 Fed. Reg. 63,720 (Nov. 9, 2007).

[3] Pub.L. 108-159 §§ 114, 315 (2003).

[4] FTC Announces Expanded Business Education Campaign on 'Red Flag' Rule, Federal Trade Commission Release (July 29, 2009).

According to the FTC this latest extension comes on the heels of the House Appropriations Committee's recent recommendation that the Commission "defer enforcement in conjunction with additional efforts to minimize the burdens of the Rule on health care providers and small businesses with a low risk of identity theft problems."[5] The FTC expects to use the next three months to "redouble" its efforts to assist small businesses and entities with a low risk of identity theft with their compliance obligations under the Rule. Many of these organizations remain uncertain about their obligations. The FTC will release additional compliance guidance shortly and a special link with additional information related to compliance by small businesses and low risk entities is expected to be placed on the FTC's Red Flags Web site.[6]

The Required Identity Theft Prevention Program

The Identity Theft Red Flag Rule applies to financial institutions and creditors and calls for them to develop and implement a written "Identity Theft Prevention Program" to detect, prevent and mitigate identity theft in connection with certain "covered accounts." The Rule also requires credit and debit card issuers to assess the validity of notifications of changes of address in conjunction with a request for a new card, and any user of consumer credit reports to implement reasonable policies and procedures when a consumer reporting agency sends a notice of address discrepancy.[7]

The question receiving most attention from industry has been whether a company has "covered accounts." According to the Rule's definition, such accounts primarily include personal accounts designed to permit multiple payments or transactions (*e.g.,* credit card accounts, mortgages, loans, etc.) and any account for which there is a foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft. Thus, although the Rule focuses on accounts held primarily for personal, household or family purposes, it also includes some business accounts where there is a risk of identity theft.

Because of the breadth of this definition, a wide variety of companies find themselves subject to the Rule. Businesses extending credit to customers to buy goods on payment terms offered by the business likely have "covered accounts." Utilities or mobile telephone services are included in this Rule because they provide services which are billed monthly in arrears. But the Rule also encompasses other entities such as restaurants which offer "house accounts" under which a prominent patron may dine and be billed monthly. Likewise, a country club permitting meals, activities or accommodations to be charged to membership accounts which are then billed monthly would be subject to this Rule.

Some of the uncertainty that has prompted the latest deadline extension relates to the fact that the Rule also applies to all health care providers and hospitals that accept insurance as payment in full or part for health care services. This is due to the FTC's determination that the acceptance of insurance by health care providers constitutes the extension of credit to the providers' patients. Therefore, those patients' accounts are considered "covered accounts", and the applicable providers are subject to the Rule.

[5] *Id.*

[6] *See* www.ftc.gov/redflagsrule (last visited July 29, 2009).

[7] *See* Federal Register, Vol. 72, No. 217, Friday November 9, 2007, at 63718.

The written Identity Theft Prevention Program ("Program") must be designed to "detect, prevent, and mitigate identity theft" in connection with those "covered accounts." Each entity's Program must be able to detect patterns, practices and certain "red flag" activities that could signal possible identity theft.[8] Programs must include "reasonable policies and procedures" to: (1) identify red flag activities for covered accounts and incorporate any newly identified red flag activities into the Program; (2) detect red flag activities; (3) respond to red flag activities that have been detected; and (4) update the Program periodically to incorporate new risks. Each Program must be dynamic and tailored to the scope and complexity of the company's particular business as well as to its past experience with and risk of identity theft.

The Rule requires approval of the Program by the Board of Directors or an appropriate committee of the board, oversight of service providers who deal with covered accounts and appropriate training. Annual reports to the Board or senior management and periodic (but at least annual) review of the red flags and the Program are also mandated.

Program Implementation—It's Not Too Late

For companies who are in the process of developing their Programs, the extended enforcement date offers a bit of breathing room. For companies that remain unsure of their obligations, there is still time to put a Program into place by the new November 1, 2009, deadline. The necessary activities will vary for each organization and will depend in large part on the organization's existing fraud detection and compliance programs and experience with identity theft. The new Rule is broad and may overlap with existing programs and practices, which can be incorporated by reference into the Program as appropriate. This reduces the need to duplicate existing policies and procedures. Companies of all sizes should assemble an interdisciplinary team of individuals to develop the Program. Expertise from the organization's business team, legal and compliance department, information technology group, fraud specialists, as well as other offices with identify theft experience, will be necessary.

For assistance with regard to data security policies and procedures or for further information, please contact:

Deborah S. Thoren-Peden (bio)
Los Angeles
+1.213.488.7320
deborah.thorenpeden@pillsburylaw.com

John L. Nicholson (bio)
Washington, DC
+1.202.663.8269
john.nicholson@pillsburylaw.com

Catherine D. Meyer (bio)
Los Angeles
+1.213.488.7362
catherine.meyer@pillsburylaw.com

Meighan E. O'Reardon (bio)
Washington, DC
+1.202.663.8377
meighan.oreardon@pillsburylaw.com

Douglas A. Grimm (bio)
Washington, DC
+1.202.663.8283
douglas.grimm@pillsburylaw.com

[8] The guideline supplement includes an illustrative list of 26 different types of red flags that financial institutions and creditors may consider incorporating into their Program.