Privacy & Data Protection | Global Sourcing

November 23, 2009

FTC Again Extends Enforcement of Identity Theft Red Flag Rule, to June 1, 2010

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

Nearly two years ago, 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 Section 114 and Section 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 FTC-regulated entities who were originally required to comply by November 1, 2008. However, FTC-regulated entities now have until June 1, 2010 to comply. This new deadline represents an extension of nearly one and a half years from the initial compliance date, and comes as Congress has raised questions regarding the breadth of the regulations and a court has excluded law firms from coverage by the rules.

Many businesses and industry groups have struggled with the question of whether they or their members should be 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 businesses under its jurisdiction to achieve compliance. On April 30, 2009, the FTC further extended the enforcement deadline to August 1, 2009 and then again on July 29, 2009, the FTC granted an additional three-month

[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).

extension, moving the deadline to November 1, 2009.[4] Just as the regulation was set to take effect, the FTC has again granted an extension of six months, setting the new compliance deadline for June 1, 2010.

The FTC has spent the time leading up to November 1st on outreach efforts to further educate and prepare entities under its jurisdiction. Previous deadline extensions focused on education were intended to provide the FTC with more time for education and businesses more time to understand the obligations. This latest extension, however, was specifically sought by the House of Representatives to provide Congress with additional time to address industry objections and to provide clarification on the broad interpretation of the term "creditors" under the Rule.[5] The Red Flag Rule has begun to receive heightened attention on Capital Hill since many feel that the compliance costs and burdens for certain small businesses do not justify the risk of identity theft posed by these organizations. Further involvement by Congress has resulted in legislation, currently being considered by the Senate, to exempt certain small businesses from the Red Flag Rule and allow other entities to apply for an exemption.[6]

Additionally, on October 30, 2009, the U.S. District Court for the District of Columbia ruled that the Red Flag Rule should not apply to attorneys at law firms.[7] The court issued the ruling on a motion for partial summary judgment in favor of the American Bar Association; a written opinion is expected in November. The court's decision, however, only applies to attorneys at law firms.

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.[8]

The question receiving most attention from industry has been whether a business 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 and mobile telephone services are included in this Rule because they provide services that are billed monthly in arrears. But the Rule also encompasses other entities such as restaurants that offer “house accounts” under which a frequent 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. Additionally, the Rule also applies

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

[5] FTC Moves 'Red Flag' Deadline to June Following Request from House Lawmakers, BNA, Inc. Privacy Watch No. 209 (November 2, 2009).

[6] H.R. 3763.

[7] Am. *Bar Ass'n v. Fed. Trade Comm'n*, No. (D. D.C. Oct. 20, 2009) (order granting partial summary judgment).

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

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.

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 designed to detect patterns, practices and certain "red flag" activities that could signal possible identity theft.[9] Programs must include "reasonable policies and procedures" to: (1) identify red flag activities for covered accounts and incorporate any newly identified flags into the Program; (2) detect those activities; (3) respond to the 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 businesses that are in the process of developing their Programs, the extended enforcement date offers a bit of breathing room. For businesses that remain unsure of their obligations, there is still time to put a Program into place by the new June 1, 2010, 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. Businesses 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 and 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

[9] 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.