FTC Again Delays Enforcement of Identity Theft Red Flags Rules, to December 31, 2010

by Catherine D. Meyer, John L. Nicholson and Meighan E. O'Reardon[1]

In 2007, six federal agencies[2] issued final Rules on Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions (FACT) Act of 2003.[3] 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."[4] 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 December 31, 2010 to comply. This new deadline, representing an extension of over two years from the initial compliance date, was requested by members of Congress to allow for time to clarify which industries should be covered by the rules. Meanwhile, a court has excluded attorneys from coverage, and the medical profession is seeking a similar exclusion.

Many businesses and industry groups have struggled with the question of whether they or their members are required to comply with the FTC's Red Flags Rules (the "Rules"). The original enforcement deadline for the Rules was November 1, 2008, but the FTC has since granted five extensions. The most recent extension, announced May 28, 2010, set the compliance enforcement date to December 31, 2010.

[1] Sean Williamson, a Summer Associate with Pillsbury, assisted with this Advisory.

[2] 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.

[3] 72 Fed. Reg. 63,720 (Nov. 9, 2007).

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

The FTC spent the time leading up to November 1, 2009, on outreach efforts to further educate and prepare entities under its jurisdiction. Previous deadline extensions were intended to provide the FTC with more time for education and businesses more time to understand the obligations. These two most recent extensions, however, were specifically sought by members of Congress to provide them with additional time to address industry objections and to provide clarification on the broad interpretation of the term "creditors" under the Rules.[5] The Red Flags Rules have 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. In October 2009, the House of Representatives passed a bill without opposition to exempt certain small businesses from the Red Flags Rules and allow other entities to apply for an exemption.[6] A similar measure was introduced in the Senate on May 25, 2010.[7]

The FTC is urging Congress to pass legislation to resolve which entities will be covered by the Red Flags Rules. If Congress passes legislation clarifying the scope of the Rules, and that legislation becomes effective before the new December 31, 2010, deadline, the FTC currently intends to begin enforcement without further delay.[8]

The Red Flags Rules in the Courts

In late 2009, the U.S. District Court for the District of Columbia ruled that the Red Flags Rules do not apply to attorneys.[9] The court found that neither the language nor the legislative intent of the FACT Act granted the FTC the authority to exercise regulatory control over attorneys.[10] Furthermore, although it was not necessary for its holding, the court noted that even if Congress had intended for the FTC to regulate attorneys under the FACT Act, the FTC's "application of the [Rules] to attorneys who invoice their clients [would] not [be] reasonable."[11]

In light of the District Court's ruling, other professional organizations are attempting to prevent FTC identity theft regulation over their industries by filing similar lawsuits. On May 21, 2010, the American Medical Association, American Osteopathic Association, and the Medical Society of the District of Columbia filed suit against the FTC in the U.S. District Court for the District of Columbia. The organizations argue that the Red Flags Rules "exceed[] the powers delegated to it by Congress," and that application of the Rules to physicians is "arbitrary, capricious and contrary to the law."[12] The FTC has agreed that it would not enforce the Rules with respect to physicians until the D.C. Circuit issues a decision in the appeal of the District Court's decision or Congress provides more explicit instructions to the FTC.[13]

[5] FTC Moves 'Red Flag' Deadline to June Following Request from House Lawmakers, BNA, Inc. Privacy Watch No. 209 (November 2, 2009); FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule, Federal Trade Commission Release (May 28, 2010).

[6] H.R. 3763.

[7] S. 3416.

[8] FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule, Federal Trade Commission Release (May 28, 2010).

[9] *Am. Bar Ass'n v. Fed. Trade Comm'n*, 671 F. Supp. 2d 64, 67 (D. D.C. 2009).

[10] *Am. Bar Ass'n v. Fed. Trade Comm'n*, 671 F. Supp. 2d 64, 82 (D. D.C. 2009). The FACT Act is the legislation under which the Rules were promulgated.

[11] *Am. Bar Ass'n v. Fed. Trade Comm'n*, 671 F. Supp. 2d 64, 83 (D. D.C. 2009).

[12] Physicians File Lawsuit on FTC's Red Flags Rule, American Medical Association Release (May 21, 2010).

[13] A Doctor and a Lawyer Walk into a Bar: Moving Beyond Stereotypes, Remarks by FTC Chairman Jon Leibowitz As Prepared for Delivery, American Medical Association House, June 14, 2010, available at http://www.ftc.gov/speeches/leibowitz/100614amaspeech.pdf (Last visited July 6, 2010).

The Required Identity Theft Prevention Program

The Identity Theft Red Flags Rules apply to "financial institutions" and "creditors," each of which is defined in the Rules, and requires them to develop and implement a written "Identity Theft Prevention Program" to detect, prevent and mitigate identity theft in connection with certain "covered accounts" (also defined in the Rules). The Rules also require 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.[14]

The question receiving most attention from industry has been whether a business has "covered accounts." According to the Rules' 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 Rules focus 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 Rules. 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 aspect of the Rules because they provide services that are billed monthly in arrears. But the Rules also encompass 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 could be subject to this aspect of the Rules. Additionally, the Rules also apply 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 Rules.

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.[15] 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 Rules require 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.

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

[15] 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.

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 December 31, 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 Rules are 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