WILMERHALE

FACT Act "Red Flag" Rules

2008-09-02

Is your company prepared to comply with the "red flag" rules implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act")? On **November 1, 2008**, those rules will require many companies to identify and respond to account activities that are possible indicators ("red flags") of identity theft (though, for some companies, enforcement of certain rules will not begin until May 1, 2009). If you think that your company is not subject to the rules, think again. **The regulations apply to banks -- but also apply to any financial institution or creditor that holds a covered transaction account** -- a broad classification that includes companies such as automobile dealers, utility companies, mortgage brokers, telecommunications companies, finance companies, and non-bank financial services that provide money market accounts. According to the Federal Trade Commission, the rules are likely to affect over 11 million creditors. In the discussion below and in a separate alert update, we offer some thoughts on the steps that these companies must take in order to comply with the "red flag" rules.

Covered Entities

The rules apply to any **financial institution** or creditor that holds a **covered account**.

- A **financial institution** is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a consumer.
- A **transaction account** is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.
- A **creditor** is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Creditors include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.
- A **covered account** is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. Covered accounts include credit card

accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A covered account is also an account for which there is a foreseeable risk of identity theft - for example, small business or sole proprietorship accounts.

Requirements

- *First*, the rules require each financial institution and creditor that holds any "covered account" to **develop and implement an Identity Theft Prevention Program** designed to prevent, detect, and mitigate identity theft in connection with new and existing accounts.
- *Second*, the rules require issuers of credit and debit cards to develop policies and procedures to **assess the validity of an address change request** when that request is followed closely by a request for an additional or replacement card.
- *Third,* the rules require users of consumer credit reports to develop policies and procedures to **respond to notices from credit reporting agencies** regarding address discrepancies.

Rules Requiring Implementation of Identity Theft Prevention Program

Rules implementing Section 114 of the FACT Act require each financial institution and creditor to design and implement a written Identity Theft Prevention Program ("Program") to prevent, detect, and mitigate identity theft in connection with certain covered accounts. The programs must be uniquely tailored to a covered entity's size, complexity, and nature of operations. However, every Program must have four essential features:

- *First*, each covered entity must ***identify*** and incorporate into its Program relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft. These red flags will vary depending on the nature of the business in question, but the rules require that they be based on the guidance provided by regulators and the covered entity's own experiences.
- *Second*, each covered entity must develop policies and procedures to ***detect*** red flags that have been incorporated into the entity's Program. The agency guidelines recommend such measures as obtaining identifying information about, and verifying the identity of, a person opening an account, and, in the case of existing accounts, authenticating customers, monitoring transactions, and verifying the validity of address change requests.
- *Third,* each covered entity must ***respond appropriately*** to any red flags that are detected, to prevent and mitigate identity theft. The guidelines recommend such measures as monitoring an account for evidence of identity theft, contacting the customer, calling law enforcement, changing any password or security device that permits account access, closing an account, etc.
- *Fourth*, each covered entity must **update** its Program periodically to reflect changes in risks to customers from identity theft, or to the safety and soundness of the covered entity.

An Appendix to the rules sets out Program development guidelines addressing: Program design,

identification of red flags, red flag detection, prevention and mitigation of identity theft, Program updates, Program administration, and other applicable legal requirements.

A supplement to the Appendix lists patterns, practices, and activities that indicate a possible risk of identity theft. Each covered entity is required to evaluate the list (which is not exhaustive) and include in its Program those red flags that are appropriate to its business. The list is separated into five categories:

- 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 or a social security number listed in the Social Security Administration's Death Master File;
- 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.

The rules also enumerate certain steps that a covered entity must take to administer its written Program. The covered entity's staff must:

- Obtain approval of the initial written Program by the Board of Directors or a committee of the Board;
- Involve the Board of Directors, a committee of the Board, or senior management in the development, implementation, and administration of the Program;
- Report, at least annually, to the Board of Directors, a committee of the Board, or senior management, on compliance with the red flag regulations;
- Train staff to implement the Program effectively; and
- Exercise appropriate and effective oversight of arrangements with third-party and affiliated service providers.

These rules apply to **all financial institutions and "creditors**" that are subject to the Federal Trade Commission's administrative enforcement of the Fair Credit Reporting Act (pursuant to 15 U.S.C. § 1681s(a)(1)). The rules also apply to many other entities regulated by the federal financial institution regulatory agencies. The rules will be enforced against the latter on November 1, 2008, and against the former on May 1, 2009.

The rules define "creditor" by reference to the Equal Credit Opportunity Act (15 U.S.C. § 1681a(r)(5)) as a person who regularly participates in a credit decision, including setting the terms of credit. This is a broad definition, and the FTC estimates that it will affect over 11 million entities. The definition includes "lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies." 16 C.F.R. § 681.2(b)(5).

- Only those financial institutions and creditors that offer or maintain "covered accounts"

must develop and implement a written Program.

An "account" is broadly defined to mean "a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes."
16 C.F.R. § 681.2(b)(1).

A "covered account" is either:

- An account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, car loan, margin account, cell phone account, utility account, or savings account; or
- Any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft.

Each financial institution and creditor must periodically determine whether it offers or maintains covered accounts.

Rules Concerning Changes of Address for Credit and Debit Cards

Beginning November 1, 2008, the rules implementing Section 114 of the FACT Act also require each financial institution and creditor that issues debit or credit cards to assess the validity of certain address change requests. An issuer of a credit or debit card must implement reasonable policies and procedures to verify a change of address in circumstances where the card issuer receives an address change request for a customer's account and, within thirty days afterward, receives a request for an additional or replacement card for the same account.

In such circumstances, the card issuer may not issue the new card unless it:

- Notifies the cardholder of the request at the cardholder's former address and provides the cardholder with a reasonable means to promptly report an incorrect address change;
- Notifies the cardholder of the address change request by another means of communication that the card issuer and cardholder have previously agreed to and provides the cardholder with a reasonable means to promptly report an incorrect address change; or
- Uses other means of evaluating the validity of the address change in accordance with the reasonable policies and procedures established by the card issuer as part of its Program to prevent, detect, and mitigate identity theft (see above).

A card issuer may satisfy its regulatory obligations by validating an address change pursuant to one of the three methods described above at any time after it receives a request for an address change. That is, validation can occur before the issuer receives the request for an additional or replacement card.

Any written or electronic notice given by a card issuer pursuant to the rules must be clear and

conspicuous and must be provided separately from the card issuer's regular correspondence with the cardholder.

These rules apply to all financial institutions and creditors that issue a debit or credit card and that are subject to the Federal Trade Commission's administrative enforcement of the Fair Credit Reporting Act (pursuant to 15 U.S.C. § 1681s(a)(1)). The rules also apply to many other entities regulated by the federal financial institution regulatory agencies, to the extent that they issue debit or credit cards.

Rules Concerning Users of Consumer Credit Reports

Beginning November 1, 2008, the rules implementing Section 315 of the FACT Act require entities requesting consumer credit reports to develop reasonable policies and procedures to respond to apparent address discrepancies.

- The FACT Act requires consumer credit reporting agencies to notify parties requesting a credit report if the address provided by the requesting party "substantially differs" from the address that the credit reporting agency has on file for the consumer.
  15 U.S.C. § 1681c(h)(1).
- In turn, an entity that requests consumer credit reports (i.e., a "report user") must develop and employ reasonable policies and procedures that are triggered when the report user receives an address discrepancy notification from a credit reporting agency. Specifically, a report user must have policies in place to:

    - Enable the report user to form a reasonable belief that a consumer report relates to the correct consumer; and
    - Reconcile the address of the consumer with the credit reporting agency (i.e., furnish to the agency an address that the report user reasonably has confirmed is accurate), in circumstances where the report user: (a) establishes a new continuing relationship with the consumer; (b) can form a reasonable belief that the consumer report relates to the consumer about whom the report user has requested the report; and (c) regularly and in the ordinary course of business furnishes information to the credit reporting agency.

Examples of reasonable policies and procedures enabling a report user to form a reasonable belief concerning a consumer's identity include:

- Verifying with the consumer the information in the consumer report provided by the credit reporting agency; or
- Comparing the information in the consumer report with information the report user:

    - Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing

31 U.S.C. § 5318(l), namely, 31 C.F.R. § 103.121;

- Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or
- Obtains from third-party sources.

The policies and procedures for address reconciliation must ensure that the report user will furnish the consumer's address as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

These rules apply to all users of consumer credit reports that, pursuant to 15 U.S.C. § 1681s(a)(1), are subject to the Federal Trade Commission's administrative enforcement of the Fair Credit Reporting Act. The rules also apply to many other entities regulated by the federal financial institution regulatory agencies, to the extent that they request consumer credit reports.

Authors

Yoon-Young Lee

SENIOR COUNSEL

yoon-young.lee@wilmerhale.com

+1 202 663 6720