Red Flags Rule and Identity Theft Prevention Programs
Ellen J. Toscano

The Federal Trade Commission (the "FTC") has delayed the enforcement of the "Red Flags" Rule (the "Rule"), designed to address the risk of identity theft, until December 31, 2010. The previous deadline had been June 1, 2010. The Rule, which was promulgated pursuant to the Fair and Accurate Credit Transactions Act (the "FACTA") and issued jointly by the FTC and the federal banking and credit union regulatory agencies, requires financial institutions and other creditors that have "covered accounts" [1] to develop and implement Identity Theft Prevention Programs, and to conduct periodic assessments to determine if they have any covered accounts. They must then develop a Program to help identify, detect and respond to patterns, practices or specific activities (or "red flags") that could be an indication of identity theft. The purposes of the Rule are to help financial institutions and other creditors identify red flags in advance so they are better prepared to spot suspicious activity, and to help protect account holders and customers from identity theft.

The FACTA Rule applies to financial institutions and other creditors that have covered accounts. FACTA defines "financial institutions" as state and national banks, state and federal savings and loan associations, mutual savings banks, state and federal credit unions, and any other person or entity that, directly or indirectly, holds a "transaction account" for a consumer. A transaction account is a deposit or other account from which the owner can make payments or transfers. It includes checking accounts, demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

A "creditor" is defined very broadly by FACTA as any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit, even if that person assigns all financing responsibilities to a third party; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. A creditor is thus basically any person or business that regularly permits, or arranges for, the deferred payment of debt. Some examples are banks, finance companies, mortgage brokers, automobile dealers and retailers that offer or arrange financing, third-party debt collectors, utility companies, telecommunications companies, and any other businesses that provide services and bill their customers later. In August of 2009, the FTC announced that some professionals, including lawyers, doctors, dentists and accountants, fall under the definition of "creditor" and are thus subject to the Rule. However, the U.S. District Court for the District of Columbia ruled on October 30, 2009 that the FTC may not apply the Rule to attorneys. The FTC is appealing that ruling. The American Medical Association is also challenging the applicability of the Rule to health care providers.

---

[1] There are two kinds of covered accounts. The first is an account used primarily for personal, family or household purposes and that involves or is designed to permit multiple payments or transactions. Examples are checking accounts, savings accounts, credit card accounts, mortgage loans, auto loans, margin accounts, cell phone accounts and utility accounts. The second is any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk of identity theft. Examples are small business accounts, sole proprietorship accounts and single transaction consumer accounts.

The Rule provides guidance for how businesses must develop, implement and administer their Identity Theft Prevention Programs. A Program, approved by the entity's board of directors or senior management must include the following four basic elements: (i) reasonable policies and procedures to identify red flags of identity theft that a business might confront in its day-to-day operations; (ii) methods for detecting the identified red flags; (iii) actions that will be taken when red flags are detected; and (iv) methods for re-evaluating and updating the Program periodically to meet changing risks.

With regard to the first element, different types of covered accounts pose different types of risk, and thus the type of account should be considered when developing a Program. For instance, red flags for accounts that are opened or accessed on-line may differ from those that involve face-to-face contact. With respect to the second element, procedures must be specified for detecting red flags in the business' daily operations, such as requiring the use of certain identity verification and authentication methods for new and existing accounts. As for the third element, a business must be prepared to respond appropriately, depending on the degree of risk posed. Examples include closing an account, not opening a new account, changing passwords and notifying law enforcement. Finally, new red flags will emerge as technology changes and identify thieves change their tactics. Thus, periodic updates are required to ensure that the Program is current with risks.

The FTC provides guidance for compliance with the Rule through materials posted on the dedicated Red Flags Rule web site (www.ftc.gov/redflagsrule). It has also published a compliance guide and created a template with an easy-to-use online form for low-risk entities to create an identity theft program.

A covered entity that fails to comply with the Rule may be subject to civil monetary penalties. Civil monetary penalties for noncompliance are currently $3,500 per violation. However, for repeated violations after an order to comply, the FTC could file a suit seeking several times that amount for each violation.