

FEDERAL IDENTITY THEFT PREVENTION REQUIREMENTS

By **BRIAN DAY**, Staff Attorney, IML

New federal regulations, known as "red flag rules", require financial institutions and creditors to develop and implement written identity-theft-prevention programs. Because of the definition of "creditor", many municipalities may be affected by these regulations.

A municipality that provides a service to customers and collects payment later must comply with the red flag rules.

The red flag rules are part of the federal Fair and Accurate Credit Transactions (FACT) Act of 2003. Under these regulations, financial institutions and creditors with covered accounts must have identity-theft-prevention programs in place by November 1, 2008 to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

A. Who Must Comply With the Red Flag Rules?

The red flag rules apply to "financial institutions" and "creditors" that have "covered accounts". To determine whether a municipality must comply with the red flag rules, the key definitions to look to are "*creditor*" and "*covered account*".

The term "*creditor*" includes municipalities that provide services to customers and, subsequently, bill for those services. Federal statute defines the term "creditor" as "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit."¹

The term "*person*" means "a natural person, a corporation, *government or governmental subdivision or agency*, trust, estate, partnership, cooperative, or association."² According to the Federal Trade Commission, "where non-profit and government entities defer payment for goods or services, they...are to be considered creditors."³

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.⁴

B. What Do the Rules Require?

The regulations require a written program that includes reasonable policies and procedures that are designed to detect, prevent, and mitigate identity theft in connection both with existing accounts and with the opening of a new account. The program must identify and detect the relevant warning signs (or "red flags") of identify theft. The program must include four basic elements:

- The identification of relevant red flags for covered accounts;
- The establishment of a process to detect those red flags;
- Appropriate responses to detected events; and
- Periodic updates to policies and procedures to reflect changes in risk exposure.

The federal rules include guidelines. The guidelines are intended to assist in the formulation and maintenance of the required identity-theft-prevention program. Each entity that is required to implement a program must consider the guidelines and include those that are appropriate. The guidelines are contained in appendix J to Part 41 of the Code of Federal Regulations.⁵

1. The identification of relevant red flags for covered accounts: The guidelines set forth five categories of red flags. The program should include relevant red flags from the following categories as appropriate:

- Alerts, notifications, or warnings from a consumer reporting agency;
- Suspicious documents;
- Suspicious personally identifying information, such as a suspicious address;
- Unusual use of – or suspicious activity relating to – a covered account; and
- Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

A supplement to the guidelines identifies 26 possible red flags.⁶ These red flags are not a checklist, but rather, are examples that entities may want to consider as a starting point.

2. Detecting relevant red flags: Items to consider in detecting red flags include:

- Obtaining identifying information and verifying the identity of those wanting to open a new account;
- Authenticating transactions for existing customers to include photo ID plus possible additional verification methods such as biometrics, tokens, security ID cards, fingerprint readers and GPS technology using cell phones. For online transactions these methods plus a user ID and passwords create a two-factor authentication process. The regulations do not specify the use of technology, they only stress the need to be “effective”.
- Monitoring customer transaction activity with special emphasis on a change of address closely followed by a new service request or a material change in a customer’s credit use. There are rules-based database scanning technologies that look for patterns and anomalies and issue an alert.
- Verify the validity of customer change of address on existing accounts in order to monitor the diversion of statements as a prelude to possible account manipulation.⁷

3. Other procedural requirements: In implementing the program, entities falling under the red flag rules must take the following steps:

- Obtain board approval of the initial program;
- Ensure oversight of program development, implementation and administration via the board or a senior manager;
- Annually report to the board or senior manager on the effectiveness of the program, an explanation of “significant events” and recommendations to program changes due to evolving risks and methods of identity theft.
- Train appropriate personnel to implement the program.
- Oversee service-provider arrangements because the “covered entity” is responsible to make sure the provider has and is following a theft-protection plan.

C. How Flexible are the Red Flag Rules?

According to the Federal Trade Commission, the red flag rules are designed to be flexible. The red flag rules provide all financial institutions and creditors the opportunity to design and implement a program that is appropriate to their size and complexity, as well as the nature of their operations. The guidelines issued by the FTC, the federal banking agencies, and the NCUA should be helpful in assisting covered entities in designing their programs.⁸

For questions concerning the red flag rules, you can contact the Federal Trade Commission at RedFlags@ftc.gov.

¹ 15 U.S.C. § 1691a(e)

² 15 U.S.C. § 1691a(f)(emphasis added).

³ FTC Business Alert, June 2008, <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm> (visited July 29, 2008).

⁴ *See id.*; *see also*, 12 C.F.R. 41.90.

⁵ 72 FR 63753, Nov. 9, 2007 (available at <http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf>).

⁶ *See id.*

⁷ *See id.*

⁸ *See* Note 3, *supra*.