

## Red Flag rule affects not-for-profit & government entities

by Thomas W. Grundy, tgrundy@bkd.com

The Federal Trade Commission (FTC) jointly with the federal banking regulatory agencies and the National Credit Union Administration (NCUA) issued a final rule on Identity Theft Red Flags and Address Discrepancies or Red Flags.

Mandatory compliance with the new rule was slated for November 1, 2008, but has been delayed until May 1, 2009.

Failure to comply can be costly. The FTC can assess civil penalties of up to \$2,500 for each violation of the rule.

### Background

The rule implements sections 114 and 315 of the *Fair and Accurate Credit Transactions Act of 2003* (FACT Act), which amended the *Fair Credit Reporting Act* (FCRA). The rule requires financial institutions and creditors that hold covered accounts to develop and implement an identity theft prevention program for new and existing accounts.

### Application of Red Flags rule to not-for-profits & government

The rule broadly defines creditor as any person who defers payment for services. Examples could be a college or university that defers payment of tuition or institutional loans to faculty, staff and students. Financial institutions are defined as banks, thrifts, credit unions and other institutions that offer transaction accounts.

Under the rule, a financial institution or creditor must determine if any of its extensions of credit are covered accounts, meaning an account primarily for personal,

family or household purposes that involves multiple payments or transactions, such as a utility account or a loan that is billed or payable monthly. The rule and the FTC's guidance state that covered accounts include certain arrangements in which an individual establishes a continuing relationship with the enterprise.

### Key components of the rule

There are three components of the rule:

**Written identity theft prevention program** – Financial institutions and creditors holding covered accounts must develop and implement a written identity theft prevention program for both new and existing accounts that includes reasonable policies and procedures to detect or mitigate identity theft and enable them to:

- ◆ Identify relevant patterns, practices and specific forms of activity that are Red Flags signaling possible identity theft

and incorporate those Red Flags into the program

- ◆ Detect the Red Flags that have been incorporated into the program
- ◆ Respond appropriately to detected Red Flags to prevent and mitigate identity theft
- ◆ Ensure the program is updated periodically to reflect changes in risks from identity theft
- ◆ Effectively administer the program and report at least annually to the board of directors

**Policies & procedures for address discrepancies** – Users of consumer reports must develop reasonable policies and procedures for an address discrepancy



*With a top 10 U.S. CPA and advisory firm, you'll gain from our broad perspective on the issues you face and **experience a clear point of view.***

---

from a consumer reporting agency. This applies when a not-for-profit or government organization uses consumer reports for credit or background checks on prospective employees or credit applicants.

**Validity of address change request –**

Debit and credit card issuers must develop policies and procedures to assess the validity of a change of address request followed closely by a request for an additional or replacement card.

**Content of the program & other considerations**

**Written program –** The Red Flags 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. Guidelines issued by the FTC, the federal banking agencies and the NCUA provide some guidance to covered entities. A supplement to the guidelines identifies 26 possible Red Flags as examples that financial institutions and creditors may want to use as a starting point. They fall into five categories:

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

**Training –** An institution covered by the rule must train staff to implement the program.

**Service providers –** When a financial institution or creditor hires a service provider to perform an activity in connection with one or more covered accounts, the financial institution or creditor should take steps to ensure the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

**Preparing for compliance**

Your board of directors must approve the initial written program prior to the mandatory compliance deadline of May 1, 2009. Consult with your legal counsel on the rule's application to your organization. Contact your BKD advisor to discuss the appropriate steps to develop and implement a conforming identity theft program.◆◆

This BKD Feature Article has been prepared for clients and professional associates of **BKD, LLP**, one of the 10 largest CPA and advisory firms in the country. The information published here is intended as a brief summary of selected recent legal developments. It is not intended to provide consulting advice and should not be relied on for that purpose. For this reason, do not rely on this information as tax advice or formal opinion or regard it as a substitute for detailed advice for your particular situation. Contact your BKD advisor for more detailed information.

---

For additional information, visit [www.bkd.com](http://www.bkd.com) or contact your BKD advisor.