

Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy

In October 2007, the Federal Banking Agencies – the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve Board (the Board), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and National Credit Union Administration (NCUA) – along with the Federal Trade Commission (FTC) jointly issued final rules on identity theft “red flags” and address discrepancies. The final rules implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. The FTC granted an additional three-month delay of enforcement requiring covered financial institutions and creditors to comply by November 1, 2009.

Under the Red Flags Rules, financial institutions and creditors must develop and implement a written Identity Theft Prevention Program that includes responses for preventing and mitigating the crime, plus a plan for Program updates and staff training.

According to a report of the President’s Identity Theft Task Force, identity theft (a fraud attempted or committed using identifying information of another person without authority) results in billions of dollars in losses each year to individuals and businesses.

The final rules require each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing and mitigating identity theft and enable a financial institution or creditor to:

- **Identify** relevant patterns, practices and specific forms of activity that are “Red Flags” (see details, below) signaling possible identity theft and incorporate those red flags into the Program
- **Detect** Red Flags that have been incorporated into the Program
- **Respond** appropriately to Red Flags in order to prevent and mitigate identity theft

- **Ensure** the Program is periodically updated to reflect changes in risk from identity theft

The final rules also require credit and debit card issuers to develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. In addition, the final rules require users of consumer reports to develop reasonable policies and procedures to apply when they receive a notice of an address discrepancy from a consumer reporting agency.

What is a Red Flag?

A Red Flag refers to a pattern, practice, or specific activity that indicates the possible existence of identity theft. Supplement A to the final rules and guidelines provides 26 examples of Red Flags for consideration when implementing the Program.

Red Flags fall into five categories:

1. Alerts, notifications, or warnings from a consumer reporting agency; suspicious documents
2. Presentation of suspicious documents
3. Suspicious personally identifying information, such as a suspicious address

LOOKING FOR MORE INFORMATION?

Additional resources can be found on the Federal Trade Commission’s (FTC) website at:

- <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>
- <http://ftc.gov/opa/2007/10/redflag.shtm>
- <http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf>

4. Unusual use of – or suspicious activity relating to – a covered account
5. Notifications or Reports from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts

Who must comply with the Red Flags Rules?

The Red Flags Rules apply to “financial institutions” and “creditors” with “covered accounts.” Under the Rules, 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. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Creditors include finance companies (credit cards), automobile dealers (auto loans), mortgage brokers (mortgages), utility companies (accounts for gas, electric, oil, etc.), and telecommunications companies (cell phone accounts). Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors (higher education – student loans and medical providers – payment accounts).

A **covered account** is an account used mostly for personal, family, or household purposes and 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.

Complying with the Red Flags Rules

Under the Red Flags Rules, financial institutions and creditors must develop and implement a written Identity Theft Prevention Program. The Program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the Program. The Program must include appropriate staff training. The organization must also report at least annually to the Board of Directors or senior management on compliance with the regulations.

The Program’s written policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected; these responses should be proportionate to the degree of risk posed.

Appropriate responses to the identification and detection of Red Flags may include the following:

- Monitoring a covered account for evidence of Identity Theft
- Contacting the customer
- Changing any passwords, security codes or other security devices that permit access to covered accounts
- Reopening a covered account with a new account number
- Declining to open a new covered account
- Closing an existing covered account
- Notifying law enforcement and filing a Suspicious Activity Report (SAR), if applicable
- Suspending or eliminating a method of accessing funds of certain accounts (i.e. fax transfers) where security procedures may have been compromised
- Declining to issue a new credit card when proceeded by a change of address or other account-information

change, unless such change is independently verified

How flexible are the Red Flags Rules?

The Red Flags Rules require a risk-based approach. Each financial institution or creditor must conduct a risk assessment in order to develop and implement a program that is appropriate to the size and intricacy of the organization and the nature and scope of its activities. In addition, the Program must allow the organization to address changing identity theft risks. The risk assessment should document a complete analysis of the identity theft risks in a succinct manner so that it can be easily shared and communicated across the organization, including to the board of directors, management and appropriate staff. Examples of risk factors that should be used to identify Red Flags include:

- Types of covered accounts the organization offers or maintains
- Methods the organization offers to open covered accounts
- Methods the organization provides to access covered accounts
- Previous experiences with identity theft

The Programs must incorporate oversight of third-party service providers to ensure regulatory

compliance on their part as well. The Guidelines issued by the FTC and the Federal Banking should be helpful in assisting covered entities in designing their programs.

How can CPAs assist their organizations?

CPAs can assist financial institutions or creditors with the Red Flags Rules by:

- Developing a risk assessment methodology and conducting a comprehensive risk assessment of the organization
- Defining and developing a written Identity Theft Red Flag Program
- Conducting independent Red Flag Program reviews to assess effectiveness of the program
- Offering training assistance

When do the Red Flags Rules go into effect?

The final rules are effective on January 1, 2008. Covered financial institutions and creditors were initially set to comply with the rules by November 1, 2008. This date has been postponed several times. The FTC has just granted an additional three-month delay of enforcement requiring covered financial institutions and creditors to comply by November 1, 2009. Read the [FTC News Release](#) to learn more.

Used with permission from the AICPA's Information Technology Center (infotech.aicpa.org)

DISCLAIMER:

This publication has not been approved, disapproved or otherwise acted upon by any senior technical committees of the American Institute of Certified Public Accountants, nor does it represent the views of or an official position of the American Institute of Certified Public Accountants. This article is not intended as legal, accounting or other professional advice and should not be relied upon as such. If legal, accounting or other professional advice or expert assistance is required, the services of a competent professional should be sought.