

# Identity Theft Red Flags & Address Discrepancies under the FACT Act of 2003

## Summary of Final Rule

On November 9, 2007, the Office of the Comptroller of the Currency (“OCC”), Federal Reserve Board (“Board”), Federal Deposit Insurance Corporation (“FDIC”), Office of Thrift Supervision (“OTS”), National Credit Union Administration (“NCUA”), and Federal Trade Commission (“FTC”) jointly issued a final rule and guidelines implementing sections 114 of the Fair & Accurate Credit Transactions Act of 2003 (“FACT Act”).

The rule requires financial institutions and creditors to develop and implement a written Identity Theft Prevention Program (“Program”) to detect, prevent, and mitigate identity theft in connection with certain financial accounts. The guidelines accompanying the final rule are designed to assist financial institutions and creditors in formulating and maintaining a Program that satisfies the requirements of the new rule.

The mandatory compliance date for these rules is November 1, 2008.

### *Who Must Comply with the New Rule?*

Under the final rule published by the Agencies, any financial institution or creditor that offers or maintains covered accounts must comply with the new rule.

#### **I. Creditors & Financial Institutions**

The final rule defines “creditor” as any person who arranges for the extension, renewal, or continuation of credit. The final rule specifically identifies mortgage brokers as being included in this definition of creditor.

#### **II. That Offer Covered Accounts**

The final rule defines “covered account” as:

- (1) An account primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions, or
- (2) Any other account for which there is a reasonably foreseeable risk of identity theft for consumers or the financial institution or creditor.

It is the responsibility of each financial institution or creditor to periodically determine whether it offers or maintains covered accounts.

Some specific examples of covered accounts cited in the rule include: credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts.

## ***What Does the New Rule Require?***

The new rule requires any financial institution or creditor that offers or maintains covered accounts to develop and implement a written Identity Theft Prevention Program (“Program”). The Program must be designed to detect, prevent, and mitigate identity theft in connection with any covered account. The Program should be tailored to the size of the financial institution or creditor, and also to the complexity of and nature of its operations.

### **I. Initial & Periodic Risk Assessments**

Before a financial institution or creditor attempts to implement any Program, it must first conduct a comprehensive risk assessment to determine whether it offers or maintains covered accounts. The financial institution or creditor should consider:

- (1) The types of covered accounts it maintains;
- (2) The methods it provides to open its accounts;
- (3) The methods it provides to access its accounts; and
- (4) Its previous experience with identity theft.

This risk assessment directs financial institutions and creditors to first determine whether they will need to develop and implement a Program under the new rule. If a Program is required, the risk assessment should help those financial institutions and creditors identify the types of Red Flags its Program needs to address. For example, certain Red Flags relevant to deposit accounts may be different than Red Flags applicable to consumer credit accounts or business accounts.

If this initial risk assessment leads a financial institution or creditor to determine that it does not need to implement a Program, those financial institutions and creditors are still required to conduct periodic reassessments of whether a Program is needed, based upon changes in the accounts it offers or maintains or other various factors set forth in the final rule.

### **II. Establishment & Maintenance of a Written Identity Theft Prevention Program**

Each financial institution or creditor that offers or maintains covered accounts must implement a written Program that includes reasonable policies and procedures to address the risk of identity theft posed to its customers or its own safety and soundness. The Program must address financial, operational, compliance, reputation, and litigation risks, and should be specially tailored to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

To provide financial institutions and creditors with greater flexibility in developing a Program that is appropriately tailored to the size, complexity, and nature of their individual operations, the Agencies offer detailed guidance in Appendix J of the final rule. This guidance is designed to assist financial institutions and creditors in the formulation and maintenance of their individual Programs.

Each financial institution or creditor is required to consider the guidelines provided in Appendix J and include in its Program those guidelines it deems appropriate. However, financial institutions and creditors are free to determine that particular guidelines in Appendix J are not appropriate for their individual operations. The guidelines in Appendix J also make it clear that a financial institution or creditor covered

by the new rule may, where appropriate, incorporate into its Program existing processes for controlling reasonably foreseeable risks of identity theft. The Agencies believe this additional provision will help financial institutions and creditors avoid unnecessary duplication and allow these entities to benefit from already existing policies and procedures.

While the guidelines in Appendix J offer financial institutions and creditors a degree of flexibility in implementing the required Program, the final rule does set forth four basic elements that must be included in every financial institution or creditor's Program.

Each Program must contain reasonable policies and procedures for:

- (1) Identifying relevant Red Flags for covered accounts, and incorporating those Red Flags into the Program;
  - a. "Red Flags" are defined as any pattern, practice, or specific activity that indicates the possible existence of identity theft.
  - b. Red Flags should be identified and incorporated from relevant sources including:
    - i. Prior incidents of identity theft that the financial institution or creditor has experienced;
    - ii. New methods of identity theft that the financial institution or creditor has identified as reflective of changes in identity theft risks; and
    - iii. Applicable supervisory guidance.
  - c. When identifying Red Flags, financial institutions and creditors must consider the nature of their business and the type of identity theft to which they may be subject.
  - d. Examples of individual Red Flags are appended to the final rule as Supplement A to Appendix J.
- (2) Detecting Red Flags that have been incorporated into the Program;
  - a. **The new rules suggest** financial institutions and **creditors** should enhance their ability to detect Red Flags incorporated in their Program by, among other things:
    - i. **Verifying the identity of individuals opening covered accounts;**
    - ii. **Authenticating the identity of customers with existing accounts;** and
    - iii. Verifying the validity of change of address requests.
- (3) Responding appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
  - a. In determining the appropriate response to Red Flags that are detected by the Program, financial institutions and creditors should consider any aggravating factors that may heighten the risk of identity theft (examples of such factors are outlined in Section IV of the guidelines included in Appendix J).

- (4) Ensuring the Program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.
  - a. Section V of the guidelines included in Appendix J identifies several factors that should cause a financial institution or creditor to update its Program, including:
    - i. The financial institution or creditor's own experience with identity theft;
    - ii. Changes in methods of identity theft;
    - iii. Changes in methods of detecting, preventing, or mitigating identity theft;
    - iv. Changes in the types of accounts the financial institution or creditor offers or maintains; and
    - v. Changes in the financial institution or creditor's business arrangements.

### **III. Administration of the Written Identity Theft Program**

The new rule also requires financial institutions and creditors to take certain steps in administrating the Program. These steps include:

- (1) Obtaining approval of the initial written Program from their board of directors or a committee of their board of directors;
  - a. For financial institutions and creditors that do not have a board of directors, approval must be obtained from a designated employee at the level of senior management.
- (2) Ensuring oversight of the development, implementation, and administration of the Program;
  - a. The final rule states that oversight should include:
    - i. Assigning specific responsibility for the Program's implementation;
    - ii. Reviewing reports, prepared at least annually, by staff concerning the compliance of the financial institution or creditor with new rules;
    - iii. Approving material changes to the program as necessary to address changing identity theft risks.
- (3) Training staff; and
  - a. Each financial institution or creditor to whom the new rules apply must train members of their staff, as necessary, to effectively implement the Program.
  - b. Training is required only for "relevant staff." However, the term "relevant staff" is not further defined.

(4) Overseeing service provider arrangements.

- a. Each financial institution or creditor to whom the new rules apply must exercise appropriate and effective oversight of service provider arrangements.
- b. The guidelines included in Appendix J explain that whenever a financial institution or creditor engages a service provider to perform an activity in connection with a covered account, the financial institution or creditor must ensure that the activity of the service provider is conducted in accord with reasonable policies and procedures for detecting, preventing, and mitigating the risk of identity theft.
- c. The guidelines in Appendix J also provide an example of how a financial institution or creditor may comply with this requirement of the rule.
  - i. A financial institution or creditor could require their service providers, by contract, to have policies and procedures in place to detect relevant Red Flags that may arise in the performance of their activities. These service providers could further be required to either report these Red Flags to the financial institution or creditor or take the necessary and appropriate steps to prevent or mitigate identity theft.

***When is Compliance with the New Rules Required?***

The mandatory compliance date for all financial institutions and creditors to whom the new rules apply is November 1, 2008.

***\* This article is for informational purposes only and does not constitute legal advice. Readers should not rely on it as such. No one should attempt to interpret or apply any law without the aid of an attorney.***