

## **IDENTITY THEFT RED FLAGS AND ADDRESS DISCREPANCY REGULATIONS**

### **Effective Date**

The federal financial regulatory agencies (Comptroller of the Currency, Federal Deposit Insurance Corporation, Federal Reserve Board, National Credit Union Administration, Office of Thrift Supervision) and the Federal Trade Commission announced final amendments to their Fair Credit Reporting Act (FCRA) regulations on October 31, 2007 to implement Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The regulations become effective on January 1, 2008 with a mandatory compliance date of November 1, 2008.

### **Background**

The agencies had previously published a proposed rule making in July 2006. The agencies received 128 written comments from financial institutions, other business groups and consumer groups. The final regulations and guidelines reflect changes made as a result of the public comments received.

### **Summary**

#### **Identity Theft Red Flags**

Each financial institution or creditor is required to periodically determine whether it offers or maintains “covered accounts” which is a defined term under the new regulations. As part of this determination it must conduct a risk assessment to determine whether it offers or maintains these types of accounts. If it does it becomes a covered institution for purposes of the regulation.

The new rules require each covered institution to establish an Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft either at the opening of a covered account or an existing covered account.

- The Program must be in writing and approved by the institution’s board of directors (or an appropriate committee of the board).
- The institution must involve the board, an appropriate committee, or a designated senior management employee, in the oversight, development, implementation and administration of the Program.
- Staff must be trained to effectively implement the Program.
- The institution must exercise appropriate and effective oversight of service provider arrangements.

A Program must include reasonable policies and procedures to:

- Identify relevant Red Flags for the covered accounts offered or maintained by the institution and incorporate those Red Flags into its Program;

- Detect Red Flags that have been included into its Program;
- Respond appropriately to any Red Flags that are detected; and
- Ensure that the Program (including relevant Red Flags) is periodically updated to reflect changes in risks to customers and to the safety and soundness of the institution from identity theft.

Institutions that are required to implement a Program must consider the following guidelines outlined in Appendix J to the regulations:

#### *The Program*

An institution may incorporate, as appropriate, its existing policies, procedures, or other methods that may control reasonably foreseeable risks to customers or to the safety and soundness of the institution from identity theft.

#### *Identifying Relevant Red Flags*

An institution should consider the following risk factors for identifying Red Flags for covered accounts:

- The types of covered accounts it offers or maintains.
- The methods it provides to open covered accounts.
- The methods it provides to access its covered accounts.
- Its previous experiences with identity theft.

The institution should incorporate relevant Red Flags from sources such as:

- Any incidents of identity theft experienced by the institution.
- Methods of identity theft that the institution has identified that reflect changes in identity theft risks.
- Applicable supervisory guidance.

The Program should include relevant Red Flags from the following categories as appropriate. Examples of Red Flags for each category are included in Supplement A to Appendix J.

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers such as fraud detections services.
- Presentation of suspicious documents.
- Presentation of suspicious personal identifying information.
- The unusual use of, or suspicious activity related to a covered account.
- Notice from customers, victims of identity theft, law enforcement authorities, or other person regarding possible identity theft in connection with covered accounts held by the institution.

#### *Detecting Red Flags*

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts by:

- Obtaining identifying information about and verifying the identity of a person opening a covered account, for example, using the institution's Customer Identification Program.
- In the case of existing covered accounts, authenticating customers, monitoring transactions, and verifying the validity of change of address requests.

### *Preventing and Mitigating Identity Theft*

Policies and procedures should provide for appropriate responses to the detection of any Red Flags commensurate with the degree of risk posed. These may include:

- Monitoring a covered account for evidence of identity theft.
- Contacting the customer.
- Changing any security devices that permit access to a covered account.
- Reopening a covered account with a new account number.
- Not opening a new covered account.
- Closing an existing covered account.
- Not attempting to collect on or not selling a covered account to a debt collector.
- Notifying law enforcement agencies.
- Determining that no response is warranted under the particular circumstances.

### *Updating the Program*

The Program (including any relevant Red Flags) should be periodically updated to reflect changes in risks to customers or to the safety and soundness of the institution based on:

- The institution's experiences with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, or mitigate identity theft.
- Changes in the types of accounts offered or maintained by the institution.
- Changes in the institution's business arrangements such as mergers, acquisitions, alliances, joint ventures or service provider arrangements.

### *Methods for Administering the Program*

Oversight of the Program should include:

- Assigning specific responsibility for the Program's implementation.
- Review of annual reports on compliance prepared by staff members.
- Approval of material changes to the Program as necessary to address changing identity theft risks.

A report regarding compliance with the regulatory requirements of the Program should be prepared by staff on at least an annual basis for review by the board of directors or appropriate designated persons. The report should address material matters such as:

- The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and existing covered accounts.
- Service provider arrangements.
- Any significant incidents involving identity theft and management's response.
- Any recommendations for changes to the Program.

Whenever an institution engages a service provider to perform an activity in connection with covered accounts, the institution should take steps to ensure that 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.

### *Other Applicable Legal Requirements*

Institutions must be mindful of other related legal requirements that may be applicable such as:

- 31 U.S.C. 5318(g) on filing Suspicious Activity Reports in accordance with law and regulations.

- Implementing any requirements under Section 605a(h) of the Fair Credit Reporting Act regarding the circumstances under which credit may be extended when the institution detects a fraud or active duty alert.
- Implementing any requirements under Section 623 of the Fair Credit Reporting Act, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate.
- Complying with the prohibitions of Section 615(f) of the Fair Credit Reporting Act on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

### **Duties Regarding Address Discrepancies**

The final rules for implementing this portion of Section 315 of the FACT Act provides that a user of consumer reports must develop and implement reasonable policies and procedures that are designed to enable it to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report when the user receives a notice of address discrepancy from a consumer reporting agency. These policies and procedures apply in connection with both the opening of an account and in other circumstances when the user of a consumer report already has a relationship with the consumer.

These requirements are subsumed into the Identity Theft Program by being included in Supplement A to Appendix J as an illustrative example of a Red Flag. Therefore, the adoption of an Identity Theft Program will also address this portion of the regulatory requirements regarding address discrepancies.

Another requirement of the regulations implementing this portion of Section 315 requires that an institution develop and implement reasonable policies and procedures for furnishing an address for the consumer that it has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when it:

- Can form a reasonable belief that the report relates to the person on whom the report was requested;
- Establishes a continuing relationship with the consumer; and
- Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which it obtained the notice of address discrepancy.

The agencies note that if the user of the consumer report cannot establish a reasonable belief that the report relates to the person about whom it has requested the report, they expect that the user will not use the report.

### **Definitions**

The following definitions are important in understanding how the new regulations may apply to your institution.

*Account* – a continuing relationship established by a person to obtain a product or service for personal, family, household or business purposes. It includes:

- An extension of credit, such as the purchase of property or services involving a deferred payment; and
- A deposit account.

*Covered Account –*

- An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
- Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

The thrust of these two definitions is to encompass a very broad sweep of transactions and services offered by various types of creditors. The inclusion of business purposes under the definition of “account” brings small business loans made to individuals under the requirements of the regulation. This is further emphasized in the definition of “covered account” by the second bulleted criterion regarding reasonably foreseeable risk to either customers or the safety and soundness of the creditor.

*Red Flag* – a pattern, practice, or specific activity that indicates the possible existence of identity theft.

This definition will require ongoing attention to existing and potential examples of identity theft. This should enhance the attention management gives to existing programs of quality control and fraud detection as well as CIP reviews as this will provide the framework for compliance with the new requirements.

**Action Plan**

- ✓ Conduct a risk assessment to determine whether the institution offers or maintains covered accounts.
- ✓ Establish an Identity Theft Prevention Program to detect, prevent, and mitigate identity theft at account opening or on existing accounts.
- ✓ Draft procedures to implement the Identity Theft Prevention Program.
- ✓ Train staff on the Identity Theft Prevention Program.
- ✓ Implement the Identity Theft Prevention Program.

**Author**

Ken Baebel, CRCM, CRP  
Director, Regulatory Relations  
November 5, 2007

Copyright 2007, Integrated Compliance Solutions, LLC