

*Who's watching your back?*

## Identity Theft Red Flags Rule Overview

### Building a Identity Theft Prevention Program

*Powell Hamilton*

# Agenda

- ▶ Regulation Overview
- ▶ Who Does it Impact?
- ▶ What is Required?
- ▶ Typical Assessment Approach
  - Risk Assessment
  - Covered Accounts
  - Identity Red Flags
  - Detection Policies and Procedures
  - Response Policies and Procedures
  - Document Prevention Protection Program
  - Staff Training
- ▶ Address Discrepancies
- ▶ Penalties for Non-compliance
- ▶ Recommended Actions

# Regulation Overview

The Fair and Accurate Credit Transactions Act of 2003 ("FACTA") final regulations regarding identity theft prevention programs have been issued. This new requirement, known as the "Identity Theft Red Flags Rule", became effective on January 1, 2008, with compliance mandatory by November 1, 2008. It will require your institution to adopt a written identity theft prevention program that gains approval from your board.

The following regulatory agencies are responsible for publishing the requirements:

- ▶ Federal Trade Commission (FTC);
- ▶ Comptroller of the Currency (OCC);
- ▶ Federal Reserve System (FRS);
- ▶ Federal Deposit Insurance Corporation (FDIC);
- ▶ Office of Thrift Supervision (OTS); and
- ▶ National Credit Union Administration (NCUA).

# Who Does it Impact?

The new regulatory requirement affects the following organizations:

- ▶ Banks
- ▶ Credit Unions
- ▶ Mortgage Companies
- ▶ Consumer Loan Companies
- ▶ Auto Dealers
- ▶ Utility Companies
- ▶ Phone Companies
- ▶ Other Creditors

# What is Required?

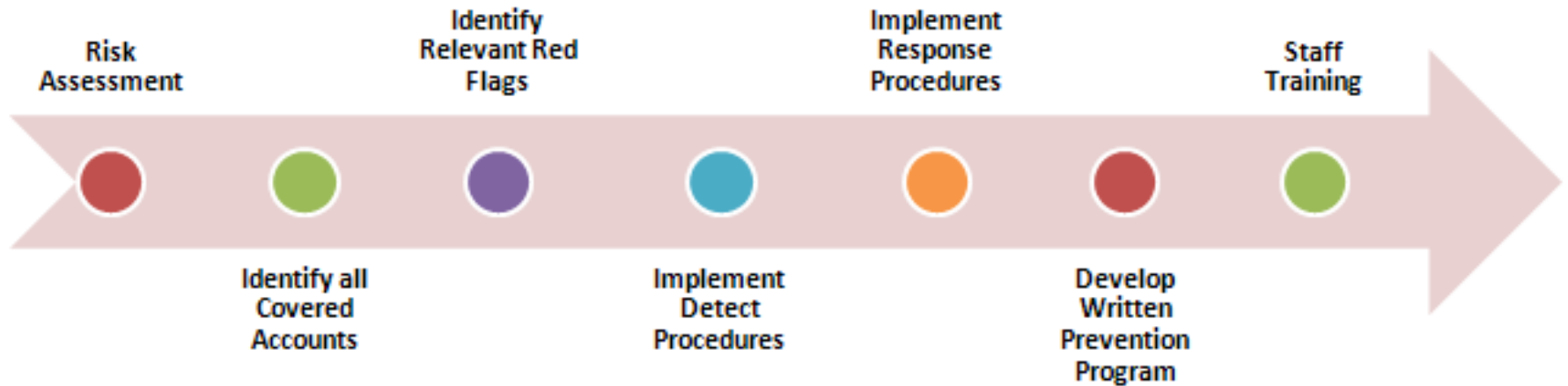
The Identity Theft Prevention Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft. The regulation requires an institution to have:

1. An established written Identity Theft Prevention Program approved by the Board of Directors;
2. Initial Risk Assessment;
3. Policies and procedures for detecting, preventing, and mitigating identity theft. Policies and procedures need to include:
  - A. Identify relevant patterns, practices, and specific forms of activity that are signals for possible identity theft;
  - B. The capability to monitor and detect “red flags” identified;
  - C. The capability to respond appropriately to any red flags and to take corrective action;
  - D. Policies and procedures to verify address changes;
4. Regular compliance reporting;
5. Oversight of service providers;
6. Mandatory staff training; and
7. Ensure the Program is reviewed periodically and is updated to reflect any changes.

# Example of Identity Theft

- ▶ Stealing Mail
- ▶ Diverting Mail
- ▶ Impersonating Victims in Person
- ▶ Intercepting Information Transmitted Electronically
- ▶ Rummaging through Trash
- ▶ Stealing Wallets – Credit Cards
- ▶ Stealing Data from the Workplace

# Typical Assessment Approach



# Initial Risk Assessment

Financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts. It will also determine the scope of the Prevention Program and the amount of effort to create this program. The following highlights key Risk Assessment tasks:

1. Determine Entity Type of the institution;
2. Identify institution assets;
3. Identify accounts offerings;
4. Identify the type of consumer accounts;
5. Determine methods it provides to open its accounts;
6. Determine methods it provides to access its accounts;
7. Assess previous experiences with identity theft issues;
8. Identifying supporting systems (i.e., network devices, servers, etc.)
9. Identify well-known risks and/or vulnerabilities; and
10. Risk analysis and documentation.

# What is a “Covered Account?”

- ▶ A “covered account” is a consumer account offered or maintained by a creditor or financial institution that involves multiple payments or transactions, such as a credit card account, mortgage loan, or checking account.

# Identity All Covered Accounts

A covered account is an account that a financial institution or creditor offers or maintains.

- ▶ Credit Card accounts
- ▶ Mortgage loans
- ▶ Automobile loans
- ▶ Margin accounts
- ▶ Cell phone accounts
- ▶ Utility accounts
- ▶ Checking or savings accounts

# Identity Relevant Red Flags

A Red Flag Identifier can be a pattern, practice, or a specific activity that triggers the belief that identity theft has occurred. Within the regulation, there are five specific Red Flag categories:

- ▶ Alerts, Notifications or Warnings from a Consumer Reporting Agency;
- ▶ Suspicious Documents;
- ▶ Suspicious Personal Identifying Information;
- ▶ Unusual Use of, or Suspicious Activity Related to, the Covered Account; and
- ▶ Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities or any other group.

# Implement Detection Procedures

The following subtopics represent categories of red flags that are used to help detect identity theft in connection with the opening of accounts and existing accounts by:

- ▶ Alerts, Notifications or Warnings from a Consumer Reporting Agency or Fraud Detection Service
- ▶ Presentation of Suspicious Documents
- ▶ Presentation of Suspicious Personal Identifying Information
- ▶ Unusual Use of, or Suspicious Activity Related to an Account

# Implement Response Procedures

It is the responsibility of all personnel to appropriately respond to events of suspected or identified cases of identity theft and red flags that are commensurate with the degree of risk posed.

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

# Develop Written Protection Program

The Identity Theft Prevention Program is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The program is based upon the size, complexity, the nature and scope of its activities. The program must be documented and must include policies and procedures to:

- ▶ Identify relevant red flags for the covered accounts that the organization offers or maintains, and incorporate those red flags into the program;
- ▶ Detect red flags that have been incorporated into the program;
- ▶ Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- ▶ Ensure the program (including the red flags determined to be relevant) is updated periodically.

# Staff Training

Training program need to provide employees with current identity theft training information (through regular updates), and a testing mechanism to ensure staff comprehension of training information and directives. Training must include the following:

- ▶ Organization's Policies
- ▶ Identified Red Flags
- ▶ Detection Methods
- ▶ Response Methods

# Address Discrepancies

- ▶ Those who use credit reports need policies and procedures to use when they receive a notice of address discrepancy from a consumer reporting agency. The user must form a reasonable belief that the report relates to the consumer and furnish a confirmed address.

# Penalties for Non-Compliance


The Red Flags Rules were published as part as the Fair and Accurate Credit Transaction Act (FACTA). Penalties applying to FACTA also apply to the Red Flags Rules.

- ▶ **Federal Trade Commission** - The FTC is also authorized to bring enforcement actions in federal court for violations. In some cases, the FTC may bring an action for up to \$2,500 in penalties for each independent violation of the rule.
- ▶ **State Enforcement** - The states are also authorized to bring actions on behalf of their residents and may recover up to \$1,000 for each willful or negligent violation. In addition, the states may recover its attorneys' fees if successful in such action.
- ▶ **Civil Liability** - Each consumer may be entitled to recover actual damages sustained from a violation. In the case of identity theft, this could very large. Consumers may be able to bring a class action suit seeking potentially massive damages. In addition, a successful plaintiff, or class of plaintiffs, may recover reasonable attorneys' fees.

# Recommended Actions

The following are recommended actions:

- ▶ Development of a risk assessment methodology and conducting a comprehensive risk assessment across all affected business lines.
- ▶ Design and develop the written Identity Theft Red Flag Program.
- ▶ Consider a independent Red Flag Program reviews to assess effectiveness of the program.
- ▶ Develop training material and incorporate it into your existing training program.
- ▶ Develop a response to identity theft incidents.



*Who's watching your back?*

## Identity Theft Red Flags Rule Overview

### Building a Identity Theft Prevention Program

*Powell Hamilton*