



Identity Theft Prevention Program (FACTA Identity Theft Red Flags Rule)

Overview

The Fair and Accurate Credit Transactions Act of 2003 ("FACTA") requirement, known as the "Identity Theft Red Flags Rule", became effective January 1, 2008, with compliance mandatory by November 1, 2008. It requires certain organizations to adopt a written identity theft prevention program approved by the Board of Directors.

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. The 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
- 7) Ensure the Program is reviewed and periodically updated to reflect changes.



10 Step Approach to Compliance

A typical approach to developing an identify theft prevention program includes:

- 1) Initial risk assessment
- 2) Identify all covered accounts
- 3) Identity relevant “red flags”
- 4) Implement detection policies and procedures
- 5) Implement response policies and procedures
- 6) Develop and document a written identify theft prevention program
- 7) Staff education and training
- 8) Gap analysis and follow-up review
- 9) Modifications to the program
- 10) Subsequent risk assessments

1. Initial Risk Assessment

The financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts. The assessment also determines the scope of the Prevention Program and the amount of effort to create this program.

The following are 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
- 10) Risk analysis and documentation

2. Identify Covered Accounts

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. Examples include:

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



3. Identify 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:

- 1) Alerts, Notifications or Warnings from a Consumer Reporting Agency
- 2) Suspicious Documents
- 3) Suspicious Personal Identifying Information
- 4) Unusual Use of, or Suspicious Activity Related to, the Covered Account
- 5) Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities or any other group

4. 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

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

5. 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
- Determining that no response is warranted under the particular circumstances



6. Develop and document a written identify theft prevention 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
- Ensure the program (including the red flags determined to be relevant) is updated periodically

7. Staff Education and Training

The training program needs 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. At a minimum, the training must include the following:

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

8. Gap Analysis and Follow-up Review

Additional investigation and research to determine “gaps” between policies and procedures and actual operations. Evaluate your organization’s risk exposure based upon information provided during the initial assessment.

9. Modifications to the Program

The identity theft prevention program should be modified over time as the organization evolves and new services are offered. The organization should review covered accounts to determine changes that require enhancements and modifications to the identity theft prevention program.

10. Subsequent Risk Assessments

Periodic risk assessments:

- Ensure the organization continues to meet compliance requirements
- Help evaluate the effectiveness of the organizations risk management mechanisms. Help reduce identity theft
- Protect the organization’s image and reputation



Publication and Author Information

Jim Kelton is Managing Principal of Altius IT (www.AltiusIT.com), an IT security audit, security consulting, and risk management company based in Costa Mesa, California. Mr. Kelton has over 30 years of experience in the Information Technology industry and is recognized as a security expert. He is certified by the Information Systems Audit and Control Association (ISACA) as:

Certified Information Systems Auditor (CISA)

Certified in Risk and Information Systems Controls (CRISC)

Certified in the Governance of Enterprise IT (CGEIT)

He sits on the Board of Directors of the following associations and organizations:

- Association of Professional Consultants (APC)
- International Association of Professional Security Consultants (IAPSC)
- Technology Professionals Association (TPA)