



Helping Your Financial Institution Address the Identity Theft Red Flags Rule



Identity Theft: A Costly and Growing Concern for U.S. Organizations

Recent updates to the Fair and Accurate Credit Transactions Act (FACTA) of 2003 require that U.S. financial institutions comply with the Identity Theft Red Flag guidelines. The guidelines state that any organization using consumer credit data is responsible for developing and implementing an effective identity theft program to include policies, procedures and tools for detecting, preventing and mitigating identity theft.

Fiserv's Identity Theft Red Flags Rule Solution

Fiserv provides an innovative, comprehensive and end-to-end solution to help your financial institution address the Red Flags Rule requirement. With Fiserv, you can effectively detect and mitigate threats on new and existing accounts, as well as lending and deposit applications, via a holistic view of your customer and any identity theft risks. From identity verification and transaction monitoring to advanced workflow and case management capabilities, Fiserv can meet your Red Flag regulatory requirements and improve the compliance and verification processes within your organization.



- Improve risk protection
- Meet Red Flag requirements
- Streamline compliance operations
- Reduce departmental costs
- Leverage a holistic approach

The Fiserv Identity Theft Red Flag Rule solution's key capabilities include:

Identity Verification

Identity verification capabilities help financial institutions during the account origination process determine if the person is who they say they are, if his/her information is linked to suspicious activity and if the person is listed on any Government Watch list;

Address Verification

Address verification services enable financial institutions to validate address change requests instantly for maximum customer responsiveness and fraud detection, eliminating the need for most manual verification processes;

Transaction and Customer Monitoring

Employs NetEconomy's comprehensive detection engine to monitor financial and customer transactions, and non financial events to generate alerts when a red flag condition exists;

Red Flag Repository

Provides a centrally managed red flag repository storing alerts from all systems including manual alerts by your staff, or automated alerts from your identity verification and transaction monitoring systems. All alerts are aggregated for a single integrated view of risk;

Workflow

End-to-end best-practice workflow allows users to configure their own workflows with built-in configuration functionality including check lists and automated alert assignment routing;

Case Management System

Built-in case management system tracks, prioritizes and manages suspicious cases, automates reporting, and records an audit trail with complete case history and detailed log of all actions taken and reports filed;

System Flexibility

Flexible system for business and regulatory change makes it easy to adjust or add new risk areas and rules as needed;

Accelerated Deployment

Leverages standard Fiserv interface for fast and easy implementation.

The Fiserv Advantage

Fiserv provides a comprehensive, integrated and superior solution to mitigate identity theft across your organization. Fiserv offers:

- Comprehensive coverage for compliance standards, monitoring every account origination request;
- Multi-faceted compliance capability addressing both USA PATRIOT ACT and FACTA Red Flags regulatory requirements;
- Highly flexible, configurable and easily deployable integrated solution offering to meet your specific requirements;
- Unrivaled data coverage for increased verification accuracy whatever size the organization; improving customer service and reducing manual reviews.

Key Elements of a "Red Flags" Program

- Identify patterns and specific forms of activity that are ID theft "red flags" and incorporate them into the program
- Program approval by the board of directors or an appropriate committee of the board
- Monitor red flags that have been incorporated into the program
- Respond appropriately to red flags that are detected to mitigate identity theft
- Ensure regular updates to the program that reflect changes in identity theft risks
- Develop procedures to assess the validity of a request for a change of address that is closely followed by a request for an additional or replacement card
- Develop reasonable policies and procedures to apply when an address discrepancy notice is received from consumer reporting agency

About Fiserv Fraud and Compliance Solutions

Fiserv provides a portfolio of integrated solutions that can be leveraged together for improved detection capabilities, fewer false positives, reduced revenue losses, and streamlined workflow. Fiserv integrates solutions from NetEconomy for anti-money laundering, customer due diligence, trade surveillance, fraud prevention and employee fraud detection; CheckFree/Fiserv Risk Solutions for ATM, Card, Check and ACH fraud mitigation, and Fiserv Imagesoft's FraudGuard for digital check imaging and protection against forgery, counterfeits and alterations.

For more information on Fiserv's FraudLink Red Flag Solution, please visit www.fiserv.com or contact your Fiserv account executive.

Fiserv Corporate Headquarters, 255 Fiserv Drive, Brookfield, WI 53045
Phone: 262-879-5000 Toll Free: 800-872-7882 www.fiserv.com