

# The Federal Reserve “Red Flag” Ruling – An Overview

Under the “Red Flag” Regulations, financial institutions must conduct an ID Theft risk assessment for their institution, and based upon that assessment, put in place a written program which includes controls to address those risks. The “Red Flag” Ruling requires that safeguards be in place by November, 2008. The Ruling requires the following:

“Red Flag” Requirements	Secure Identity Systems Provides
Initial Risk Assessment	✓
Policies and Procedures Manual	✓
Train Staff on Program Implementation	✓
New Account Authentication (All consumer accounts)	✓
Validate Change of Address Requests (All consumer accounts)	✓
Anti-Phishing Program	✓
Identity Theft Protection (All consumer accounts)	✓

***Secure Identity Systems is the only company in the country that has the “end to end” solution for the new “Red Flag” ruling.***

## ***Initial Risk Assessment***

The risk assessment required per 12 CFR Part 41 Subpart J (c) determines if an institution has covered accounts that it must develop a formal ID Theft Prevention Program for. The risk assessment must be updated periodically based on changes in methods used to open accounts, methods available to access accounts, and the institution’s experience with Identity Theft. Our solution will meet these requirements.

## ***Policies and Procedures Manual***

All policies and procedures are required to be in writing and have the respective financial institution’s Board approval. The Secure Identity Systems’ Compliance Manual not only meets this requirement, but includes a Board Resolution Template as well. The manual includes updates, as required to identify changing risks, changes in methods of Identity Theft and methods to detect, prevent and mitigate Identity Theft.

## ***Train Staff on Program Implementation***

We provide onsite and web-based training to employees as part of our service. At all of our trainings, employees will receive printed materials and FAQs to help them learn about Identity Theft and the Program benefits.

## ***New Account Authentication***

Verifies the identity of a person opening a new account. It will alert the user if data cannot be verified, or if Identity Theft is suspected. It will target those accounts exhibiting the most risky behavior and provide the necessary information for additional investigation.

## ***Validate Change of Address Requests***

Our solution will verify the validity of change of address requests. It will search billions of records to look for address discrepancies and provide a score to the end user representing the risk of the address change.

## ***Anti-Phishing Program***

Secure Identity Systems provides the best anti-phishing detection and takedown service available in the market, and is currently being used by companies such as ING and the IRS. Secure Identity Systems not only monitors an institution’s website, letting them know when someone attempts unauthorized usage, but with the institution’s permission, will do a takedown of any fraudulent website.

## ***Identity Theft Protection***

Secure Identity Systems solutions employ three patented technologies to deliver unparalleled anti-fraud and authentication weapons. From the monitoring of the total identities of a financial institution’s account holders to the assignment of a personal Resolution Advocate to assist in the event of a theft, Secure Identity Systems ensures a seamless end-to-end solution for your institution.