



---

## **Getting Compliant: The 7 Step Red Flags Checklist**

**Bryan Ansley, CEO, Secure Identity Systems**

**Republished from Bankers Digest**

The clock is ticking. On November 1...financial institutions are required by the Federal Reserve to meet key Red Flag rule requirements or face potential sanctions and monetary penalties. Banks are now scrambling for solutions only to find that [many] of the available tools address only a subset of the Fed's regulation. Many financial institutions need to step back and make a careful evaluation of the regulations' implications. There's still time to create a plan.

The reason for the new regulation is simple: identity crime is spiraling out of control. FBI statistics show United States companies spend \$67 billion annually combating cyber crime; and consumers lose \$50 billion to identity theft and recovery expenses every year, according to the Federal Trade Commission. Regulators know that banks can play a pivotal role in the fight against identity fraud by implementing the new regulatory requirements.

The Red Flag regulations require all financial institutions to implement identity theft protection programs to include "reasonable policies and procedures" for preventing identity theft and the ability to track "red flag" activities and notify victims. Compliance with the comprehensive regulation can be addressed by implementing the seven measures detailed in the following Red Flags Checklist.

### **Initial Risk Assessment**

The risk assessment required per 12 CFR Part 41 Subpart J (c) determines if an institution has covered accounts and a formal ID Theft Prevention Program. The risk assessment must be updated periodically based on changes used to open accounts, methods available to access accounts, and the institution's experience with identity theft.

### **Policies and Procedures Manual**

All policies and procedures are required to be in writing and to have the respective financial institution's board approval. The proper manual not only meets this requirement, but includes a board resolution template as well. The manual includes updates, as required, to identify changing risks and changes in methods of identity theft and strategies to detect, prevent and mitigate identity theft.

### **Staff Training on Program Implementation**

A requirement of the ruling is to increase operational efficiencies while decreasing fraud risk. To ensure this regulation is met, a program should ideally provide onsite and web-based training to employees.

### **New Account Authentication**

Financial institutions will also be required to implement tools to validate change of address on all accounts. Institutions must be able to identify the level of risk associated with address changes and react accordingly. New technologies now enable institutions to search through a database with more than 700 million records receiving over 4 million updates per month: the result is the most accurate information in the industry. This technology also flags individuals who are “highest probability” matches, and reduces the false positive rate by over 20 percent by utilizing authentication practices.

### **Validation of Change of Address Requests**

An effective Change of Address Verification tool should identify the level of risk associated with address changes. The 700-million-strong database described under “New Account Verification,” is also available for use in the case of changes of address requests. Such a request could trigger an exhaustive search through a database with more 700 million records receiving over four million updates per month to reflect literally the entire mortgage and deed-record base, along with the monthly changes taking place: the result can be the most accurate information in the industry. The Change of Address Verification tool should also flag individuals who are “highest probability” matches. When implemented correctly, best-in-class authentication practices, reduce the false positive rate by over 20 percent.

### **Anti-Phishing Program**

Phishing attacks have risen dramatically in the last year and have significantly undermined trust in online commerce. Under the new regulation, financial institutions must have an anti-phishing program in place. Companies such as ING and the IRS are currently using the best anti-phishing detection and takedown service available in the market. Institutions can now access these world-class tools to protect their customers.

### **Identity Theft Protection**

Lastly, financial institutions must provide all consumer accounts with some level of identity theft protection. According to Unisys Corporation’s Annual ID Theft Survey, up to 50 percent of consumers said they would switch their financial institution for one that offered better protection against identity theft. This is an area where institutions can not only increase their customer base but also generate substantial non-interest income by providing a higher-level of protection through proven strategies.

### **The Deadline is Approaching**

Before the November 1, 2008, deadline banks must implement a sound identity theft program addressing the seven areas outlined in the regulatory requirements. Ensuring these safeguards are in place will prevent costly compliance issues and will protect bank’s customers from identity fraud.

For more information, visit [www.secureidentitysystems.com](http://www.secureidentitysystems.com), or contact the company by phone: (615) 377-7661 or e-mail: [bansley@secureidentitysystems.com](mailto:bansley@secureidentitysystems.com).