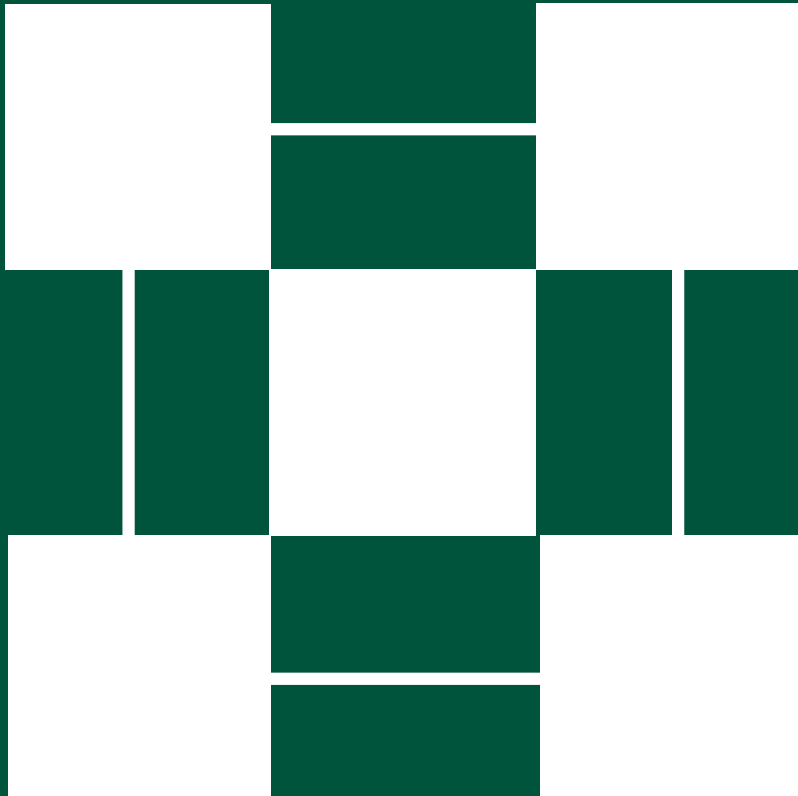


ID Theft Red Flags and Address Discrepancies Implementation Experiences



**MBA Residential Technology
Steering Committee (ResTech)**

Information Security Subgroup

December 2008

I. Introduction

A. Background

The trend for increased regulatory guidance in financial services continues with the latest Federal requirements for Identity Theft Red Flags and Address Discrepancies. This Rule's primary focus is fraud mitigation, but the regulation will affect a wide range of practices throughout organizations. Businesses must assess the risk to any account that permits multiple payments or transactions, establish a program to mitigate those risks, and institute administrative oversight.

The OCC, Board, FDIC, OTS, NCUA and FTC (the Agencies) are jointly issuing final rules and guidelines implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) and final rules implementing section 315 of the FACT Act. The rules implementing section 114 require each financial institution or creditor to develop and implement a written Identity Theft Prevention Program (Program) to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts.¹

A revealing aspect of these rules is that they expand the definitions of "credit" to include any deferral of payment and "creditor" to be anyone who participates in the credit decision. Both of these definitions increase the scope of responsibility for mortgage industry participants. This includes not only loan payment accounts, but also transactional business account. If a business invoices its clients for services monthly, allowing deferred payments, then these accounts receivable may constitute "Covered Accounts" under the regulation. A key requisite of the Rules is the inclusion in the Program of a list of the organization's identity risks to Covered Accounts, and the appropriate actions to prevent and mitigate these threats.

Another new tendency of regulations is to put the burden of oversight and administrative activities on the organization. Responsibility for establishing a Program is placed on the organization's Board of Directors, senior management, and management. There are requirements for annual reporting to management on the results of the Program, periodic reviews of the Program, and supervision of Service Providers supporting those accounts.

The rules contain two parts: Identity Theft Red Flag and Address Discrepancies. The latter, Address Discrepancies Notification, is new and requires businesses to establish procedures to respond to notifications received from credit bureaus.

¹ [Uhttp://www.nacubo.org/x10804.xml](http://www.nacubo.org/x10804.xml)U - Office of the Comptroller of the Currency, Treasury (OCC)

These notifications, "Address Discrepancies Indicators (ADIs)" require due diligence from organizations to identify the reason for the notice, perform actions based on that reason, and potentially report the findings to the credit bureau.

B. MBA Position

For the past several years, the MBA has urged organizations to establish comprehensive risk programs. Creation of such programs necessitates a holistic review of an organization's financial, fraud prevention, and security controls. Implementing unique programs to comply with each individual regulatory rule is inefficient and extremely expensive. Discussions with member companies have confirmed that implementation of the Red Flag requirements is more about tweaking existing fraud prevention programs than creating any new initiative. The identification of an organization's risk profile specific to Red Flags is new; however, the written Program, detection and response processes, and administrative oversight can be folded into current controls.

C. Scope

In the following sections, authors from various mortgage lending process areas relate their experiences with implementing the regulation. This paper shares the lessons learned by industry professionals as they ensured that their organizations were in compliance with the Identity Theft Red Flags and Address Discrepancies regulations. Note that this is not a compliance guide for Federal regulations or business partner requirements. Neither is it a substitute for legal advice. Readers should consult with qualified legal counsel regarding the compliance and legal requirements of their organizations.

II. Lender Perspective

A. Assessment

The identification of our covered accounts was straightforward (all mortgage loans) and many of the Red Flag indicators were included in our existing Mortgage Loan Processing Standard Operating Procedures. The basic governance and compliance processes for enforcement were already in place. In practice, we did not view the Red Flag requirements as a new program, but as an enhancement of processes within our existing Compliance/Fraud/Security programs.

Our assessment indicated we were already adhering to the Spirit of the rule--our overall risk was low--however, we uncovered some minor gaps that were related to Address Validation and the administration and documentation of the Red Flag Program:

1. Address Validation

The need to enhance the address validation process to include notification to credit reporting agencies.

2. Clarification of GLBA/Security vs. Red Flag/Fraud Detection

We concluded that most of our security controls and processes should be considered preemptive complements to, and not replacements or material components of, Red Flags.

3. Service Provider Responsibilities

We identified the Who, What, When, Where and How of our third party service providers as these related to Red Flags attestation of compliance, notification, and contractual language.

4. Tracking and Reporting of "Red Flag Ruling" Violations

We needed to uniquely identify Red Flag exceptions for tracking and reporting purposes.

B. Implementation Approach

Our next steps to ensure compliance included:

1. Performance of a risk assessment to identify and document our Covered Accounts, business model, and existing vulnerabilities and controls.
2. Documentation of the Program and attainment of governance approval.
3. Enhancement of the Red Flag procedures.
 - a. Identification and inventory of relevant Red Flags (Source and Categories),
 - b. Incorporation of relevant missing Red Flags and Address Validations into ongoing detection processes,

- c. Modification of our Response Plan, and
- d. Tracking and reporting on Red Flag exceptions.
- 4. Development of requirements for Service Providers.
- 5. Performance of ongoing administration and training.

C. Program Administration

We determined that the following ongoing maintenance activities would be required:

- 1. Detecting, logging, escalating and resolving identified Red Flag exceptions.
- 2. Monitoring transactions (including address changes) in new and existing accounts.
- 3. Periodically monitoring the Program for changes in scope--which could include new covered accounts or red flags--legislation, and effectiveness.
- 4. Reporting to the Board on exceptions, risks, and Program effectiveness.
- 5. Providing ongoing Red Flag training and awareness to management and staff.
- 6. Binding third parties and service providers to compliance.

III. Service Provider Perspective

A. Assessment

When we became aware of the Identity Theft Red Flag legislation, we worked with our legal counsel to determine how we, as a service provider, would need to comply with its requirements. . We determined that our business units might maintain Covered Accounts, may be issuers of credit, or perform processes that include events that could fall into one of the five Red Flag categories:

1. Notifications, alerts, or warnings from a consumer-reporting agency,
2. Suspicious documents,
3. Suspicious personally identifying information,
4. Unusual use of, or suspicious activity relating to, a covered account, and
5. Notices from consumers, victims of identity theft, or law enforcement.

We began to receive requests for Attestation of Compliance with the Identity Theft Red Flag Legislation from our lender customers during the summer of 2008. Our Corporate Information Security and Compliance Office (CISO) continued to research the areas of the legislation with which our business units would need to comply.

We found that our Standard Operating Procedures already dictated that we follow many of the Fraud and Identity Theft protocols required by the current legislation for reporting any Red Flag incidents.

B. Implementation Approach

1. Identity Theft Prevention Program

We developed our Identity Theft Prevention Program to meet the following objectives:

- a. **Identify** relevant Red Flags for Covered Accounts,
- b. **Detect** Red Flags that appear in Covered Accounts,
- c. **Respond** appropriately to detected Red Flags, and
- d. **Ensure** the Program is updated periodically.

2. Red Flag Policy and Standard

Our Corporate Compliance Officer developed a Red Flag Policy and Standard. The Policy was approved by our Board of Directors and the standard was approved by the operating group executive management teams.

3. Red Flag Risk Assessment

We deployed a Red Flag Risk Assessment company-wide to allow our business units to identify the relevant red flags for their covered accounts.

4. Red Flag Workshop

CISO held a comprehensive Red Flag workshop that included our Compliance and Information Security Officers. In the workshop, we reviewed the Policy, Standard, Red Flag Overview document and training materials with our business units. We walked the business units through the Red Flag Risk Assessment and offered guidance on how to complete it. The CISO Program Office will review the completed Risk Assessments and their findings will address both corporate wide and business process requirements.

5. Red Flag Training

Our mandatory online Information Security Awareness training addresses many of the points suggested for Red Flag training, such as complex passwords, social engineering, and phishing. We developed a new Red Flag training module to address the specific Red Flag risks and reporting procedures. The training program, policy, and standard are available on our company Intranet.

C. Challenges

1. Unclear Legislation Scope

The scope of the legislation requirements that pertain to service providers is very vague. CISO attended numerous Webinars, studied white papers, and conducted research to find what appeared to be the preeminent way to implement a comprehensive and compliant program.

2. Identifying Covered Business Units

In order to address the challenge of identifying areas within our business units that were covered by the Identity Theft Red Flag regulations, we developed a Risk Assessment for the business units to use to determine which specific areas of the regulations pertained to the business services they provided to our clients.

3. Specifying Red Flag Reporting

With the existing Fraud and Identity Theft programs already in place in our individual business units, we needed to develop an enterprise-wide tracking mechanism for reporting the Red Flags to the Senior Management team.

D. Program Administration

1. Red Flag Identification and Reporting

When a business unit identifies a Red Flag, the business unit representative will submit an Information Security Action Report. CISO will review the Action Reports immediately and store them on a secure portal. CISO

maintains the contact information for reporting Red Flags and communicates the information to our lender customers. CISO will report to the Board of Directors any significant Red Flags on an annual basis. CISO also will review the training program annually and make any necessary adjustments. Any newly identified risks will be added to the training program.

2. Red Flag Requirements and Service Offerings

All of our Risk Assessments and client requests for Red Flag Attestation services are funneled through our centralized sales center. Our Client Services Manager, who is a CISO member, will compile the requirements and assess their scope. These requirements will be reported to the Executive Management team for review and approval to include them as upgrades to our Red Flag program.

IV. Compliance Technology Perspective

A. Assessment

Our Red Flag assessment included a comprehensive review of the three regulatory requirements: 1) Identity theft prevention, 2) Address discrepancies, and 3) Issues with new and existing covered card accounts.

1. Identity Theft Prevention / New and Existing Covered Card Accounts

The Red Flag detection guidelines for new and existing accounts prescribe:

Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program (CIP) rules.

Therefore, the use of a CIP verification solution to detect identity theft Red Flags is a logical option. This created an opportunity for us to extend our existing comprehensive CIP platform to include FACT ACT Red Flag compliance rules in addition to Patriot ACT, and Bank Secrecy Act and Anti-Money Laundering (BSA/AML) requirements.

2. Address Discrepancies

The second key piece of our evaluation centered on address discrepancy and account behavioral monitoring requirements. Here, we were able to extend the existing anti-fraud monitoring platform to include specific rules and measures for Red Flag compliance. As a result, the solution now provides automated compliance verification in support of several regulations, thereby enhancing the platform's value to our customers.

B. Implementation Approach

Our approach was to extend our existing CIP, anti-fraud and case management solution to create a comprehensive Red Flag solution. The existing modules were based on proven technologies capable of supporting many customers and scaling to their growing needs. The ability to expand the scope of the solution to meet these new regulatory requirements enabled us to provide additional value to existing clients without the need for new technical integrations.

The solution monitors all account and employee activity in real time and provides automated alerts on identify theft activities such as name, address, or account beneficiary changes that are of a suspicious nature. Our software's behavioral monitoring capability can detect common patterns of this kind of activity that often are difficult to differentiate from normal business activities. Sometimes employing an automated system can generate "false positive" alerts, which our system helps manage.

Finally, to help sift through the volumes of data and alerts to differentiate between false positives and real identify theft, an integrated case management services platform enhances the tracking and management of identity theft cases while facilitating the productivity and workflow of reporting and filing. The case management module facilitates collection of Red Flag detection data from the CIP and anti-fraud modules while keeping case information organized and up-to-date and providing an enterprise view of cases exhibiting any type of fraudulent activity.

C. Challenges

During our initial assessment, we reviewed the twenty-six Red Flag examples and evaluated how to quantify each requirement in order to detect warnings using automated software. During this evaluation, we encountered several challenges, described below.

1. Customer Configurations

The first challenge was to configure the investigation of relevant Red Flag warnings to work within the financial institution's defined workflow. Because the relevant Red Flags can differ for each customer, we enlisted a flexible, rules-based architecture that is easily extensible to support each financial institution's policies and procedures.

2. Baseline Normal Activity

The second challenge was to establish a baseline of normal or expected activity for each relevant Red Flag rule in order to trigger suspicious activity warnings. We employed a variety of data collection methods, including direct integration options, batch processes, alerts and reports from external sources, and direct data collection over a network-sniffing device. As the data is collected, it is organized into defined measures to establish patterns of expected behavior. Examples include the number of deposits, withdrawals, ATM transactions, and overall account transactions over a defined period of months.

3. Leveraging Technology to Support Manual Verification

One final challenge was to determine how to leverage technology to provide technical support for the manual verification requirements of Red Flag detection. Our goal was to create a comprehensive Red Flag solution, so we included a data collection process to catalogue details of identification sources in support of rules like "*photo or ID information is not consistent with the appearance of the applicant.*" We also complemented manual verification processes with automated tests like identity verification and identity authentication to quantify applicant details more precisely.

D. Program Administration

Because fraud scenarios are constantly evolving, it is important for the Red Flag library to be flexible and extensible. As fraud schemes change, Red Flag rules must be enhanced to support the institution's policies and procedures. An integrated rules engine enables the financial institution to adjust existing business policies and measures easily and to incorporate requirements based on new fraud alerts. In addition, a configurable workflow helps to manage investigation, escalation, and alerts and supports changing policies and procedures. The final piece is to provide visibility for management into the effectiveness of the CIP. Results of the complete Red Flag program effort, including identification, detection, investigation, and updating component details, can be summarized in ad-hoc and custom management reports.

V. Conclusion

For best results, view the implementation of Red Flags requirements as extensions to your existing comprehensive financial, fraud prevention, and security programs. These rules, like other regulations, are not isolated, but complementary. Update your policies and procedures, train your personnel, and evaluate your current technology. The level of effort required will depend on your organization's "Risk Profile" Assessment—that is, the evaluation of the organization's number of Covered Accounts, related business processes and staff, and ability to automate controls. All good programs include three elements: people, processes, and technology. A Program to comply with Red Flag and Address Discrepancies rules is no exception. Depending on your organization's Risk Profile, your Program may touch all three or rely more heavily on one element than the others.

A major requirement is for administrative responsibility. You must generate and maintain written results of the Risk Profile Assessment and Identity Theft Prevention Program. Your Program must be approved by senior management, reviewed periodically, reporting by your Service Providers and training of personnel.

For organizations just now planning their implementations, personnel training may be the best course of action. As the regulation matures, you can seek vendor solutions for automated operational controls, management, and reports.

A couple of final notes for any organization:

- Establish an interdisciplinary team, not just legal or compliance departments. Have a full representation of all departments.
- Regulators will use a similar approach to the FFIEC Strong Authentication rule. Organization should make a good faith effort, timely (start early), involvement of appropriate staff and have a portion up and running as soon as reasonable.
- In most cases, procedures for the Gramm-Leach-Bliley Act (GLB) will cover a good deal, but this regulation will require additional ID theft procedures.
- Update the program on regular intervals and report to board.
- Train appropriate personnel and not the entire staff.
- Service Providers are any entities that provides services directly to business and touches Covered Account (open, maintain, process transactions).