In 2003, Congress passed the Fair and Accurate Credit Transaction Act (FACTA) as an amendment to the Fair Credit Reporting Act (FCRA). FACTA (Section 114) mandated the federal banking agencies and commissions to establish what is commonly referred to as the Red Flags Rule, which was implemented in 2008. The Federal Reserve Bank (FRB) has since promulgated it as part of Regulation V. The rule is both a consumer protection and a safety and soundness regulation based on the concept of using red flags to detect and prevent identity theft. Along with continual identification and integration of the institution’s experiences with identity theft, banks are expected to develop and implement a written Identity Theft Prevention Program (ITPP) utilizing the 26 red flag examples listed in the Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation (Appendix J of Regulation V).

With identity theft as a growing area of regulatory focus, it’s important to take a closer look at your program. Is it sitting on a shelf collecting dust, or is it hard at work protecting both consumers and your institution’s safety and soundness? To have a fully compliant and robust program, you must be continually aware of current developments with identity theft and have a full understanding of the rule. Your bank’s program should adapt to experiences with identity theft and perpetually re-evaluate alignment with the rule to enhance the program and minimize this threat to both consumers and your institution.

IN 2003, Congress passed the Fair and Accurate Credit Transaction Act (FACTA) as an amendment to the Fair Credit Reporting Act (FCRA). FACTA (Section 114) mandated the federal banking agencies and commissions to establish what is commonly referred to as the Red Flags Rule, which was implemented in 2008. The Federal Reserve Bank (FRB) has since promulgated it as part of Regulation V. The rule is both a consumer protection and a safety and soundness regulation based on the concept of using red flags to detect and prevent identity theft. Along with continual identification and integration of the institution’s experiences with identity theft, banks are expected to develop and implement a written Identity Theft Prevention Program (ITPP) utilizing the 26 red flag examples listed in the Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation (Appendix J of Regulation V).

With identity theft as a growing area of regulatory focus, it’s important to take a closer look at your program. Is it sitting on a shelf collecting dust, or is it hard at work protecting both consumers and your institution’s safety and soundness? To have a fully compliant and robust program, you must be continually aware of current developments with identity theft and have a full understanding of the rule. Your bank’s program should adapt to experiences with identity theft and perpetually re-evaluate alignment with the rule to enhance the program and minimize this threat to both consumers and your institution.

**Red Flag Basics**

The Red Flags Rule covers any financial institution or creditor, including banks, investment firms, loan companies, auto dealers, telecommunications providers, utilities, or other entities with “covered accounts.” An account is considered covered when it is designed to permit multiple payments or transactions or where there is a foreseeable risk of identity theft. This may include credit cards, deposits, trading accounts, margin accounts, automobile loans, mortgages, mobile phone accounts, utilities, and, in some cases, business accounts. Business accounts are “accounts” if they establish a continuing relationship between a person and a financial institution or creditor to obtain a product or service for business purposes. The FCRA definition of a person, found at 15 U.S.C. §1681a(b), is not limited to individuals. Each financial institution or creditor must determine if any of its business accounts present a reasonably foreseeable risk of identity theft under the definition of a “covered account.” According to the Federal Trade Commission, the accounts of small businesses or sole proprietorships may be particularly...
Identity Theft Red Flags

Regulatory Timeline

2003 FACTA signed into law including provisions for establishment of the Red Flags Rule
2008 The Red Flags Rule takes effect with delayed FTC enforcement
2010 FTC clarifies the definition of creditors/covered entities, enforcement begins
2013 SEC and CFTC publish regulations for investment firms

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 of possible identity theft from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution;
6. Other red flags based on the financial institution’s fraud and experience. Examples are provided in the guidelines for all but the sixth category. It is up to the bank to identify and expand upon that category based on the types of products it offers, its various points of vulnerability, identity theft experiences, and anticipated fraud schemes. Many of the red flags may already be required for your institution based on other FCRA requirements and in place by complying with the Customer Information Program (CIP) requirements of the USA PATRIOT Act. However, these should also be referenced in your ITFP.

Note: Italicized text in this feature is from the regulation; the non-italicized are the author’s remarks.

1. There are three types of alerts:
   a. Active duty alert (stays on file for 12 months);
   b. Initial alert (stays on file for 90 days); and
   c. Extended alert (stays on file for seven years).
2. Active duty and initial alerts can be cleared by either contacting the consumer as instructed by the alert, or by taking reasonable steps to verify the consumer’s identity and ensure that the request was not the result of identity theft.
3. Extended alerts must be cleared only by contacting the consumer as instructed by the alert or by contacting the consumer in person. This will ensure that the request was not the result of identity theft. Alternatively, a consumer can contact the consumer reporting agency to remove the alert;
4. "User of a consumer report" includes the "creditor" to include only entities engaged in the credit relationship; or
5. Other information on the identification is not consistent with information provided by the consumer report.

Suspicious Personal Identifying Information

1. The personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
   a. The address does not match any address in the consumer report (same as red flag 3); or
   b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration’s Death Master File.

2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correla-

Case In Point

In a recent Industry Call on Suspicious Activity Report (SAR) data analysis, the Federal Deposit Insurance Corporation (FDIC) indicated a 15 percent increase in check fraud from 2012 to 2013. This was partially attributed to password compromises in the 2012 LinkedIn and Twitter hacking attacks and customers that reuse their email login and password for their online banking. Once the fraudster accesses a bank account, he or she often looks for cleared check images to support their counterfeiting operation. One way that banks can prevent this type of fraud would be the use of blurring or truncation technology for account numbers and other sensitive images available online. Strong password and multifactor authentication controls are also necessary.
**Identity Theft Red Flags**

### Suspicious Documents

- F1 Alert
- F2 Freeze
- F3 Address Discrepancy
- F4 Activity
- F5 Forged Identification
- F6 Physical Appearance
- F7 Physical Identification Information
- F8 Internal Identification Verification
- F9 Paper Application
- F10 Bankcard Identification Verification
- F11 Identification Inconsistency
- F12 Fraud Match
- F13 Fraud Indicator
- F14 Duplicate SSN
- F15 Duplicate Address/Phone
- F16 Incomplete Application
- F17 Identification Mismatch
- F18 Authentication Questions
- F19 COA/Card Request
- F20 Transaction Patterns
- F21 Account Performance Patterns
- F22 Use of an Inactive Account
- F23 Bad Address on an Active Account
- F24 Missing Statements
- F25 Unauthorized Charges

### Suspicious Personal Identifying Information

- F26 Fraud

### Unusual Use of, or Suspicious Activity Related to, the Covered Account

- F27 Accounts where there is a reasonably foreseeable risk to customers (including business accounts) or the safety and soundness of the financial institution or creditor.

### Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons

- F19 Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution

### Quick Reference

- **Alerts, Notifications, or Warnings from a Consumer Reporting Agency or Service Provider (such as a fraud detection service):**
  - 1. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor.
  - 2. The personal identifying information provided is of a type commonly associated with fraudulent activity, as indicated by internal or third-party sources used by the financial institution or creditor.
  - 3. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
  - 4. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
  - 5. The address on an application is the same as the address provided on a fraudulent application, or the phone number on an application is the same as the number provided on a fraudulent application.
  - 6. A material change in telephone call patterns in connection with a cellular phone account
  - 7. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage, and other relevant factors).
  - 8. Mail sent to the customer is repeatedly returned as undeliverable, although transactions continue to be conducted in connection with the customer's covered account

### Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons

- **Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution:**
  - 26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any person that it has opened a fraudulent account for a person engaged in identity theft.
  - 27. The financial institution or creditor is notified by a person regarding suspicious activity, unusual use of, or victims of identity theft

### Unusual Use of, or Suspicious Activity Related to, the Covered Account

- 21. A covered account is used in a manner that is not consistent with established patterns of activity on the account.
  - For example:
    - Nonpayment when there is no history of late or missed payments;
    - A material increase in the use of available credit;
    - A material change in purchasing or spending patterns;
    - A material change in electronic fund transfer patterns in connection with a deposit account; or
    - A material change in telephone call patterns in connection with a cellular phone account

### Suspicious Documents

- 19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card, a cell phone, or the addition of authorized users on the account.

### Suspicious Personal Identifying Information

- 20. A material change in telephone call patterns in connection with a cellular phone account

### Unusual Use of, or Suspicious Activity Related to, the Covered Account

- 24. The financial institution or creditor is notified by a customer that the customer is not receiving paper account statements.

### Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons

- 25. A new revolving credit account is used in a manner commonly associated with known patterns of fraud.

### Suspicious Personal Identifying Information

- 18. Keep going in your pursuit of red flags! The 26 red flag examples, identify relevant red flags considering:

### Step 1: Identify your covered accounts

- Consumer accounts designed to permit multiple payments or transactions (e.g. credit card, cell phone, utility, checking, and savings) account

### Step 2: Using the 26 red flag examples, identify relevant red flags considering:

- The types of accounts offered; the methods to open an account; the methods to access an account; previous experience with identity theft; service provider arrangements; and data breaches.

### Checkpoints

- Contemplate and cross reference all points of vulnerability (in person, ATM, mobile, online, mail, phone, wire, etc.) and service providers (third-party providers)
- Prepare and assess control documentation for each red flag and be prepared to explain to the Risk Assessment

**The Red Flags Rule requires institutions to conduct a periodic risk assessment to determine if they have covered accounts and to assess each of the red flags in the guidelines. For red flags that are deemed not applicable or proven to be ineffective, the risk assessment should provide a reasonable justification including any supporting analysis. For example, red flag 1 through only applies to users of consumer reports, red flag 19 is only required for card issuers, and red flag 20 is for revolving credit accounts. The risk assessment must also encompass relevant service providers. Specific requirements are discussed further on.

**Step 1: Identify your covered accounts

- Consumer accounts designed to permit multiple payments or transactions (e.g. credit card, cell phone, utility, checking, and savings) account

**Step 2: Using the 26 red flag examples, identify relevant red flags considering:

- The types of accounts offered; the methods to open an account; the methods to access an account; previous experience with identity theft; service provider arrangements; and data breaches.

**Checkpoints

- Contemplate and cross reference all points of vulnerability (in person, ATM, mobile, online, mail, phone, wire, etc.) and service providers (third-party providers)
- Prepare and assess control documentation for each red flag and be prepared to explain to the Risk Assessment

**The Red Flags Rule requires institutions to conduct a periodic risk assessment to determine if they have covered accounts and to assess each of the red flags in the guidelines. For red flags that are deemed not applicable or proven to be ineffective, the risk assessment should provide a reasonable justification including any supporting analysis. For example, red flag 1 through only applies to users of consumer reports, red flag 19 is only required for card issuers, and red flag 20 is for revolving credit accounts. The risk assessment must also encompass relevant service providers. Specific requirements are discussed further on.

**Step 1: Identify your covered accounts

- Consumer accounts designed to permit multiple payments or transactions (e.g. credit card, cell phone, utility, checking, and savings) account

**Step 2: Using the 26 red flag examples, identify relevant red flags considering:

- The types of accounts offered; the methods to open an account; the methods to access an account; previous experience with identity theft; service provider arrangements; and data breaches.

**Checkpoints

- Contemplate and cross reference all points of vulnerability (in person, ATM, mobile, online, mail, phone, wire, etc.) and service providers (third-party providers)
- Prepare and assess control documentation for each red flag and be prepared to explain to
IDENTITY THEFT RED FLAGS

a regulator why certain red flags may not be applicable (i.e. don’t use credit reports, don’t issue cards, etc.); • Contemplate any other red flags and incor- porate them into the risk assessment, and • Initiate control enhancement efforts as needed (gap remediation).

Maintain a Written Identity Theft Prevention Program

Unless you belong to a brand new bank, you should be able to leverage an existing program and control environment as something to build off of. This program should be re-evaluated an- nually (or more often as necessary) and updat- ed based on the risk assessment described above and include some key components to meet the various provisions of the rule, including: • Detection of red flags at all points of vulner- ability, including processes to detect red flags at account origination and for existing ac- counts (ongoing). • Responses to red flags in order to prevent and mitigate the occurrence of identity theft. These efforts should be driven by a goal of minimizing consumer impact, as well as the risk exposure to your institution. For con- sumers that become victims, provide tools and assistance to help restore their identity, accounts, and creditworthiness. Appropriate responses to red flags include: • Monitoring an impacted account; • Contacting the customer; • Changing passwords or other access controls; • Changing account numbers; • Declining an application; • Closing an account; • Not collecting on or selling a debt; • Notifying law enforcement; and • Determining that no response is warranted under particular circumstances. • Prevent identity theft and losses by maintain- ing strong authentication and Know Your Customer (KYC) controls, educating custom- ers and staff, and staying on top of fraud trends with an adaptable and learning program. • Service Provider Oversight is a significant requirement for the program. It involves identifying each service provider that handles relevant processing of covered accounts and ensuring appropriate oversight. For this, con- sider vendors that manage customer interac- tions and points of vulnerabilities, vendors that provide red flag detection services, and affiliates that act in a service provider capac- ity. Also consider business partners, brokers, and dealers where there is a hand-off of the customer application or relationship. The guidelines indicate an example of compli- ance with this provision would be to update contracts to ensure that each service provider maintains its own TFP and/or participates in your bank’s program. Either way, use the risk assessment to ensure that each service provider’s program is aligned with the internal program. Also, develop reporting from each relevant service provider to support the ongoing risk assessment and board reporting. When challenged by an auditor or examiner, the program owner should be able to readily describe red flag expectations for any given service provider and provide evidence of any monitoring or testing controls.

Board of Directors Involvement is required and indicates the priority that regulators have placed on combating identity theft and the level of accountability that is expected. Very few regulations are board-reportable and this regulation should be near the very top of your compliance priorities. Thus, an appropriate committee of the board or a designated senior manager is permissible for ownership of the program, which shows some flexibility. The board must person- ally approve the initial program, but the designated committee or senior manager is appropriate for ongoing oversight. The board or designee is responsible for ensuring an independent review of the program, though the compliance or audit department can be called upon to handle this function. Also, the board (or designee) must receive, review, and approve annual reporting which covers: • Compliance with the Red Flags Rule; • Effectiveness of the program; • Service provider arrangements; • Management response to significant inci- dents; and • Recommendations for updating the program.

Program Development should include ef- fective training for relevant employees (not just another CBT), but minimally ensure that all employees have top of mind knowledge of the program’s existence. A CBT may be appropriate for enterprise-level awareness, but something more rigorous is needed for customer facing staff and fraud operations. Comprehensive reporting should support the annual risk assessments, board reporting, and drive updates to the program. When the risk assessment is conducted, consider new business units, portfolios, joint ventures, ser- vice providers, origination channels, access points, and types of accounts. Reassess red flag relevancy, considering new fraud experi- ences and trends and techniques. Continue to adapt, identify, and incorporate new red flags. The program must be appropriate in scale proportionate to the size and complexity of the financial institution.

So, if your program has been gathering dust, it’s time to make it a priority. The requirements clearly outline that there’s expectation for an annual review and the board oversight requires emphasis the high-profile nature of this regulation. Data breaches, suspicious activity reports (SARs), and complaint activity may steer regulatory attention towards your bank. Be ready with a bullet-proof program. Besides, having a strong and adaptive program is the right thing to do for your customers and to pro- tect your institution.

ABOUT THE AUTHOR:

MATT STORER is a privacy compliance manager for Capital One. He has more than 18 years of industry experience, mostly in the area of general compliance and the privacy discipline. Storer holds a United States’ Certified Information Privacy Professional (CIPP/US) certification from the International Association of Privacy Professionals, a bachelor’s degree in business from Eastern Oregon University, and a master’s degree in management and organizational leadership from Warner Pacific College. Storer is based in the Portland, Ore. area. Reach him at matthew.storer@capitalone.com.

Endnotes

3 FDIC report: Examining the Fraud Landscape, BITS Fraud Working Group conference call, (July 10, 2013)

Leverage Your Data to Limit Credit Risk

Today, banks need to use data to improve sales, increase profitability and provide transparency in the small business and commercial credit underwriting process. CreditQuest® provides tools to capture and leverage data to efficiently perform financial analysis, determine risk ratings and actively manage the entire portfolio.

• Commercial Credit Origination
• Financial Statement Analysis
• Risk Rating Automation
• Portfolio Management
• Executive Reporting

www.harlandfinancialsolutions.com/Leverage4

800-815-5592

© 2014 Harland Financial Solutions, Inc. All Rights Reserved. CreditQuest is a registered trademark of Harland Financial Solutions. Read this answer sheet through http://faa.dba.com

Data-driven Credit and Portfolio Analysis

Visit us in booth #205 at the ABA National Community Bankers Conference.