



The Red Flags Rule: what it means for your organization

Byline: Stan Oliai, Senior Vice President, Experian's Fraud and Identity Solutions Group

Many have heard of the Red Flags Rule and know that businesses need to make changes to comply with these rules. However, understanding a few details and having a route to compliance can help an organization meet the rules quickly and effectively while also enhancing business operations.

In October 2007, the federal banking agencies, the National Credit Union Administration and the Federal Trade Commission published the final Identity Theft Red Flags and Address Discrepancies Rules under the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). These rules and guidelines effectively implement sections 114 and 315 of the FACT Act. Section 114 is intended to establish reasonable procedures that 1) assist creditors and financial institutions in identifying identity theft and 2) set forth provisions specifically applicable to debit and credit card issuers who receive notice of a customer's change of address. Section 315 requires users of credit reports to establish reasonable procedures for handling a notice of a significant discrepancy between a credit report and application for credit for covered accounts.

These rules and guidelines became effective on Jan. 1, 2008. Full institutional compliance is required by Nov. 1, 2008.

Rules, guidelines or suggestions?

A "Red Flag" may be defined as a pattern, practice or specific activity that indicates the possible existence of identity theft. At first glance, this definition can be overwhelmingly broad or ambiguous to some institutions. Fortunately, the Red Flags Rule actually provides financial institutions with the flexibility to implement risk-based programs with few mandatory requirements.

The drafting agencies anticipate that many institutions already have implemented some best practices in identity theft detection and prevention. As such, institutions may include in their Program those practices already in place to control reasonably foreseeable risks of identity theft. The published Red Flags Rule guidelines include 26 illustrative examples of possible patterns, practices and forms of activities creditors should consider when implementing a written Identity Theft Prevention Program.

While institutions are not required to implement any predetermined number of the 26 Red Flag examples, they should consider those that are applicable to their business processes, consumer relationships and risk levels.

In general, creditors should focus on identifying Red Flags for account openings, existing accounts and new activity on an account that has been inactive for two years or more. Some provisions of the guidelines are mandatory, including the following:

- Each institution must create, and keep updated, a written Identity Theft Prevention Program that outlines the steps it will take to detect and prevent identity theft
- Institutions are required to confirm that the consumer reports they request from credit reporting agencies are related to the consumer with whom they are doing business

- Institutions must review discrepancies in addresses

What types of consumer accounts and relationships are covered?

Perhaps the most common question posed in the marketplace today regarding Red Flags is one of identifying which consumer accounts and relationships are covered by these guidelines. Broadly defined, the following types of consumer accounts are covered by the Red Flags Rule guidelines:

- An account that a financial institution or creditor offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account or savings account
- Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks

Source: e-CFR Data 3/20/2008 Title 16: Commercial Practices PART 681—IDENTITY THEFT RULES 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

Compliance with the Red Flags Rule

The recently issued Red Flags Rule guidelines require each financial institution and creditor that holds any covered consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement both a written and operational Identity Theft Prevention Program. This Program should be applied to both new and existing consumer accounts. The Program must include reasonable policies and procedures for detecting, preventing and mitigating identity theft while enabling a financial institution or creditor to:

- **Identify** relevant Red Flags for the business and incorporate those Red Flags into the written Identity Theft Prevention Program
- **Detect** Red Flags that have been incorporated into the written Program
- **Respond** appropriately to any Red Flags that are detected
- **Update** periodically the Identity Theft Prevention Program to reflect changes in risk to customers and to the safety and soundness of the business from identity theft

An institution's Identity Theft Prevention Program should be updated based on experiences with identity theft as well as changes in:

- Known methods of identity theft
- Viable methods to detect, prevent and mitigate identity theft
- The types of accounts offered or maintained
- Business arrangements, including mergers, acquisitions, alliances, joint ventures and service provider arrangements

The "Program," as referenced in the official document, refers to the self-prescribed system of checks and balances that each organization implements to comply with the rules. The goal of the provisions is to drive organizations to put into place a system that identifies patterns, practices and forms of activities that indicate the possible existence of identity theft. The provisions are not

designed to steer the market to a “one size fits all” compliance platform. In essence, how businesses choose to meet the requirements will depend on the business size, operational complexity, customer transaction processes and risks associated with each of these characteristics.

“The rules are actually quite flexible in terms of program specifics. Organizations are encouraged to implement risk-based programs based on their operating dynamics,” said Anne Fortney, Partner, Hudson Cook law firm. “One of the few logistical requirements is that the Program be in written form. This is not only for potential audit purposes, but also to drive adherence and consistency to the Program.”

Rather than implementing a “rules-based” Identity Theft Prevention Program (one in which particular Red Flags are identified, detected and used in isolation or near isolation in decisioning), many institutions are opting to approach Red Flags compliance from a “risk-based” perspective. This “risk-based” approach assumes that no single Red Flags Rule or even set of rules provides a comprehensive view of a consumer’s identity and associated fraud risk. Instead, a “risk-based” systematic approach to consumer authentication employs a process by which an appropriately comprehensive set of consumer data sources can provide the foundation for highly predictive fraud prediction models in combination with detailed consumer authentication conditions (such as address mismatches or Social Security number inconsistencies).

A risk-based fraud detection system is one that allows institutions to make consumer relationship and transactional decisions based not on a handful of rules or conditions in isolation, but on a holistic view of a consumer’s identity and predicted likelihood of associated identity theft.

Many, if not all, of the suggested Red Flag rules in the published guidelines are not “silver bullets” that provide assurance of the presence or absence of identity theft. A substantial ratio of false positives will comprise the set of consumers and accounts being reviewed as having met one or more of the suggested Red Flags Rule conditions. These rules and guidelines are intended neither to prevent legitimate consumers from establishing relationships with institutions nor create a burdensome and prohibitive volume of consumer “referrals.” While those rules incorporated into an institution’s Identity Theft Prevention Program must be addressed when detected, a risk-based system allows for an operationally efficient method of reconciliation in tandem with identity theft mitigation.

In an ever-increasingly competitive marketplace, “consumer experience” has become a primary focus for many businesses. An Identity Theft Prevention Program that promotes a positive and nonintrusive consumer experience will leave businesses with a competitive advantage and hopefully improve customer acquisition and retention rates.

Some businesses will determine that they already meet most or all of their perceived requirements under the new guidelines. Some will assess the need for only minor or moderate adjustments or simply the establishment of a written Program to articulate processes already in place. Other businesses will likely need to conduct a thorough audit to identify gaps in their current fraud detection and consumer authentication system, requiring them to develop and implement a program from the ground up.

Most businesses likely fall into the second category — processes are in place for identity theft protection, but a thorough review is needed to ensure complete compliance. This presents a unique opportunity — a chance to not only improve essential operational processes, but also to streamline those processes and procedures by taking stock of industry best practices, products and services available for how to best achieve compliance.

Organizations need to act now to achieve compliance by Nov. 1, 2008. That may require working with an outside party to identify the gaps and bridge them with proven fraud detection and prevention systems.

Fraud detection and prevention systems

It is essential that institutions identify appropriate and effective fraud detection and prevention systems that also can help meet compliance obligations. Such products and services must be able to authenticate consumer identities in real time using accurate and current data sources. Elements to consider include access to consumer credit and noncredit data assets, detailed consumer identity information, measurably predictive analytics, decisioning ability and knowledge-based authentication. For many institutions, the ability to implement such fraud detection tools into existing internal or consumer-facing platforms is a critical success factor.

Experian[®] is a trusted third party and credit reporting agency that can provide consumer authentication tools based on credit and/or noncredit data sources. Through Red Flags–relevant products such as Precise IDSM, clients are notified of consumer alerts, victim statements and freezes, and suspicious personal identifying information that includes name, address, Social Security number, phone, and date of birth mismatches, inconsistencies or misuse. Experian's Credit Services and Decision Analytics business offers a series of Red Flags–relevant products and services that combine:

- Consumer credit and noncredit data assets
- Detailed consumer identity information
- Flexible delivery options
- Targeted identity theft and consumer authentication scoring models
- Custom and best-practice decisioning
- Knowledge-based authentication (interactive consumer question-and-answer sessions)
- Varied integration options, including XML or Web user interfaces

All of these products and services support our clients in creating and delivering an appropriate and measurably effective Identity Theft Prevention Program.

Platforms such as Experian's Precise ID offer clients a comprehensive risk-based approach to fraud detection. Precise ID provides clients with a single point of access to, and integration of, the aforementioned capabilities.

A case study

DealerTrack[®] is a leading provider of on-demand software and data solutions for the U.S. automotive retail industry. DealerTrack needed to find a new tool to help dealers respond to, and comply with, the Red Flags guideline.

"We knew we needed to conduct a gap analysis, and we also knew we needed someone with expertise in fraud detection and fraud detection systems to help us do it efficiently and quickly," said Strati Papageorge, Director, Product Development, DealerTrack. "We turned to Experian to help us perform an audit of our current processes, procedures and systems."

Following a month of effective collaboration with Experian, DealerTrack identified both gaps within its current system as well as opportunities to provide the market with a robust, measurably effective and appropriate Red Flags tool.

Ultimately, DealerTrack was looking for a comprehensive system that could perform consumer identity verification while leveraging broad-reaching, comprehensive data sources to deliver detailed results, targeted analytics and hosted decisioning. The tool needed to balance effective fraud detection with straightforward interpretability upon delivery.

Institutions, including auto dealers, obviously need to comply with the Red Flags guideline. In doing so, however, they also must solve the problem of making decisions quickly and consistently for all their customers.

“We’ve implemented Experian’s Precise ID as a foundational piece of our DealWatch™ solution for dealers,” said Papageorge. “Our goal was to automate as much of the identity verification process as possible and create a comprehensive system that would detect a variety of fraudulent practices and allow dealers to confidently do business with consumers within Red Flag compliance parameters.”

Precise ID assesses risk for first-party fraud, third-party fraud, synthetic identity and other consumer-based fraud patterns. The platform provides flexibly configured output schemes and incorporates a hosted decision engine so that users, such as DealerTrack and its affiliated dealers, can apply their unique situational requirements and Red Flags-compliant policies to the fraud detection process.

Conclusion

As November 2008 rapidly approaches, institutions must act now to ensure that they are establishing Red Flag-compliant practices. They must review their current accessible data sources and procedures to uncover any potential compliance gaps. Many businesses then may need to seek out and assess the necessary tools and resources to help fill in those gaps. At this point, it is recommended that institutions be well on their way toward completing their written Identity Theft Prevention Program for ultimate board-level approval. Such programs should be designed to detect, prevent and mitigate identity theft in connection with “covered accounts” and be appropriate to the size, complexity, nature and scope of business activities.

Red Flags Rule compliance presents an opportunity for businesses and organizations to take stock of their current identity theft detection and prevention tools and processes. While every covered institution must have a written and operational Identity Theft Prevention Program, each program undoubtedly will be tailored to a specific market segment, addressable consumer base and risk associated with consumer interactions. Many currently employed systems will likely be augmented with more robust and predictive tools to deliver fraud risk management, compliant processes and positive consumer experiences in tandem.

A comprehensive system will deliver the following:

- Broad-reaching and accurately reported data sources
- Targeted analytics
- Detailed and summary-level consumer authentication results
- Flexibly defined decisioning strategies and link analysis

A robust Identity Theft Prevention Program will resonate with consumers. “Today, everyone is aware of identity theft, data breaches and the need to protect personal information,” said Fortney. “Organizations that build a reputation for data integrity and consumer protection will likely see the benefits in terms of customer retention, loyalty and even the bottom line.”