

Red Flags Rule

Experian and Hudson Cook, LLP
Includes sample policies and procedures



Arguably, compliance with the Identity Theft Red Flags and Address Discrepancies Rules under the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) is the hottest topic of 2008 across many markets, including, but not limited to, financial institutions, retailers, auto dealers, telecommunications and utilities. Undoubtedly, the topic is top of mind with the vast majority of compliance officers, risk and fraud managers, and executive leadership.

Each institution covered under these guidelines finds itself at a different milestone in the overall process of adopting both a written and operational Identity Theft Prevention Program (“Program”). The intent of this paper is to assist these institutions in their efforts to comprehend the guidelines and apply them to an operationally compliant Program.

The Red Flags guidelines are designed to allow institutions flexibility, for the most part, in their interpreted implementation of a Program that is “appropriate to the size and complexity of its business and the nature and scope of its activities.”¹ Depending on one’s perspective (glass half-full or half-empty), the ability to make operational a proportionate Program can be either liberating or daunting.

This paper is intended as a resource for institutions that are at any stage in their process of complying with the Red Flags guidelines. Even institutions that feel they are fully compliant should find value in this document via additional concepts and best practices that may apply even after Nov. 1, 2008, as Red Flags compliance is not a one-time event in 2008. As such, attention and resource allocation to related efforts will not cease after Nov. 1. The paper will review the guidelines themselves, provide some insight on common challenges faced by the market, explore the concept of a risk-based approach to compliance, discuss Experian’s suite of Red Flags–relevant services, and provide a sample policies and procedures document.

Experian® takes a collaborative approach to assisting clients in their efforts to fight fraud and ensure compliance with a multitude of regulations. In tandem with Hudson Cook, LLP, we hope to provide the market with additional concepts and suggestions that will afford an opportunity to reduce costs, preserve positive consumer experiences, satisfy regulatory requirements and, of course, detect fraud.

¹*Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003*

The Red Flags Rule — an overview

Introduction

In October 2007, the federal banking agencies, the National Credit Union Administration and the Federal Trade Commission (collectively, the “Agencies”) 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, among other things, Section 114 of the FACT Act. The section is intended to establish reasonable procedures that (1) assist financial institutions and creditors in identifying and preventing identity theft (the “Red Flags Rule”) and (2) set forth provisions specifically applicable to debit and credit card issuers that receive notice of a customer’s change of address.

The Red Flags Rule became effective on Jan. 1, 2008. Full institutional compliance is required by Nov. 1, 2008.

What is a Red Flag?

A “Red Flag” is “a pattern, practice, or specific activity that indicates the possible existence of identity theft.” It is purposely broad, the intention being to cast a wide net. Fortunately, the Red Flags Rule provides financial institutions and creditors with significant flexibility in their compliance efforts, allowing them to focus on the Red Flags that are relevant to their specific businesses. Furthermore, financial institutions and creditors will be judged not on their use (or lack of use) of any particular Red Flag as an indicator of potential identity theft, but rather on the overall effectiveness of their enterprise-specific Program. This focus naturally suggests implementing risk-based tools within the framework of the Red Flags Rule’s mandatory elements.

The Agencies anticipate that many institutions already have implemented some best practices in identity theft detection and prevention. In fact, depository institutions subject to the “know your customer” rule promulgated under Section 326 of the USA PATRIOT Act, requiring such institutions to implement Customer Identification Programs (“CIPs”), are encouraged by the Red Flags Rule to incorporate relevant and effective policies and procedures from their CIP into their Programs.

The Red Flags Rule includes 26 illustrative examples of possible Red Flags financial institutions and creditors should consider when implementing a written Program. While implementation of any predetermined number of the 26 Red Flag examples is not mandatory, financial institutions and creditors should consider those that are applicable to their business processes, consumer relationships and levels of risk.

² *Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003*

The Red Flags Rule — an overview

The Red Flags Rule requires financial institutions and creditors to focus on identifying Red Flags applicable to their account opening activities, existing account maintenance, and new activity on an account that has been inactive for two years or more. Some mandatory requirements include:

- Keeping a current, written Identity Theft Prevention Program that contains reasonable policies and procedures to identify, detect and respond to Red Flags, and keeping the Program updated
- Confirming that the consumer reports requested from consumer reporting agencies are related to the consumer with whom the financial institution or creditor are doing business
- Reviewing address discrepancies

Who is subject to the Red Flags Rule?

The Rule applies to “financial institutions and creditors” who originate and/or maintain “covered accounts.” “Financial institutions” are:

- State or national banks
- State or federal savings and loan associations
- Mutual savings banks
- State or federal credit unions or
- Any other persons who, directly or indirectly, hold a “transaction account” belonging to a consumer

A “transaction account” is a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. This includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers and share draft accounts.

“Creditors” are:

- Any persons who regularly extend, renew or continue credit
- Any persons who regularly arrange for the extension, renewal or continuation of credit or
- Any assignees of an original creditor who participate in the decision to extend, renew or continue credit

This term includes banks, finance companies, mortgage brokers, utility companies, telecommunications companies, auto dealers, and just about any other retailer who finances the sale of goods or services.

The Red Flags Rule — an overview

“Covered accounts” include:

- Accounts 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.
- A collection agency is subject to the rule to the extent it is a “creditor” that maintains covered accounts. It is almost a certainty that some collectors will be creditors, e.g., those that purchase debt outright. To the extent third-party collectors or servicers are providing services to a particular creditor, they would be treated as service providers to the actual creditor and subject to whatever contractual requirements the creditor imposes with regard to red flag compliance.
- Banks and other depository institutions are considered “financial institutions” and generally subject to the rule. Whether retirement accounts or trust accounts are covered depends on whether they meet the definition of “covered account.”

So, while the primary focus of the Red Flags Rule is on consumer accounts, the second prong of the definition of “covered account” makes it clear that there may be commercial accounts at risk for identity theft as well — for example, a sole proprietorship or a commercial account with a personal guarantee.

Mandatory elements

Introduction

The Red Flags Rule requires financial institutions and creditors to establish and maintain a written Program designed to detect, prevent and mitigate identity theft in connection with their covered accounts. The Program is a self-prescribed system of checks and balances that each financial institution and creditor implements to reach compliance with the Red Flags Rule. 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 Red Flags Rule — an overview

A compliant Program must contain reasonable policies and procedures to address four mandatory elements:

- Identifying Red Flags applicable to covered accounts and incorporating them into the Program
- Detecting and evaluating the Red Flags included in the Program
- Responding to the Red Flags detected in a manner that is appropriate to the degree of risk they pose and
- Updating the Program to address changes in the risks to customers, and to the financial institution's or creditor's safety and soundness, from identity theft

Identifying Red Flags

The Red Flags Rule recognizes that a “one size fits all” approach to designing and implementing a compliant Program would not promote the objectives of the rule. Accordingly, the Red Flags Rule provides guidance as to what should be considered when crafting policies and procedures to identify Red Flags and when actually identifying the Red Flags relevant to your business.

Risk factors. A compliant Program should take into account several factors, as appropriate. Following the Agencies' guidelines published with the Red Flags Rule, financial institutions and creditors may want to consider:

- **The types of covered accounts offered or maintained.** There are various types of accounts that may be offered by a financial institution or creditor that are subject to the protections of Red Flags Rule. These can include deposit accounts, credit card accounts, loan accounts, lines of credit, installment sale accounts, etc. Any account that provides for access to funds, whether a loan or deposit account, may be a target for identity thieves. Some accounts will be more appealing targets during the account opening process (e.g., a loan or installment sale transaction); others will have appeal during the term of their existence (e.g., a deposit account, credit card or line of credit). In the latter instance, demand accounts and open-end credit accounts may be subject to the most danger from identity theft. Closed-end credit accounts may have little appeal to identity thieves after origination because it is difficult, if not impossible, to obtain additional funds without refinancing the transaction.
- **The methods you use to originate covered accounts.** In many instances, the customer will be physically present during at least some aspect of the account origination process. Preliminary inquiries and documentation requirements aimed at authenticating the customer's identity are relatively standard, and financial institutions and creditors have the added benefit of being able to observe the customer's demeanor for signs of abnormal nervousness or other questionable behavioral characteristics. If originating covered accounts via the telephone or Internet, using third-party fraud detection services and challenge questions, i.e., ones to which the answers would not be readily apparent from information in someone's wallet or consumer report, will help address the lack of physical contact with the customer. Many times, these identification processes can be seamlessly integrated into the online or telephone application process.

The Red Flags Rule — an overview

- **The methods through which you allow access to covered accounts.** Financial institutions and creditors that service their accounts and allow customer access to account information (e.g., in person, via the Internet, over the phone, etc.) must craft reasonable policies and procedures that will prevent and mitigate the potential for identity theft as a result of such account access. As mentioned above, some accounts will be more at risk for identity theft than others (established open-end and deposit accounts are more appealing to identity thieves than established closed-end accounts), and the policies and procedures should reflect the differing risks.
- **Previous experiences with identity theft.** Financial institutions and creditors should carefully assess their prior experiences with identity theft and include the red flags they identify during such assessment in their Programs. These red flags are likely to appear in future identity theft attempts and not considering their inclusion may be hard to defend.

Sources of Red Flags. Financial institutions and creditors should include in their Programs a policy and procedure requiring that they look to multiple sources when identifying red flags relevant to their enterprises. The Rule provides that these sources can include:

- **Prior incidences of identity theft.** These experiences are likely to help financial institutions and creditors identify the most common red flags that pose a risk to their businesses. In some instances, they also will recognize more sophisticated red flags. The more relevant red flags a financial institution or creditor can identify and include in its Program, the less likely it is that those red flags will survive scrutiny in the account opening or maintenance processes.
- **Methods of identity theft that reflect changes in identity theft risks.** Identity thieves can be very clever and will constantly refine their methods to increase their success. Financial institutions and creditors may become aware of these new methods in a variety of ways, e.g., trade associations, regulatory agencies, periodicals, the Internet, etc. A Program's policies and procedures for identifying red flags should provide for reassessment of applicable red flags as new information becomes available.
- **Applicable supervisory guidance.** Financial institutions receive a significant amount of guidance from their regulators, including information on known identity theft methods. The Federal Trade Commission has Web pages dedicated to identity theft issues, and many state supervisory agencies provide information to their regulated entities as well. Good policies and procedures will address the need to review the information a financial institution or creditor may receive from its regulator, as well as other easily accessible regulatory guidance.

Categories of Red Flags. The Red Flags Rule provides that financial institutions and creditors should include relevant red flags in their Programs from five specific categories, as appropriate. These are:

- Alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services

The Red Flags Rule — an overview

- Suspicious documents presented by the customer
- Suspicious personal identifying information presented by the customer
- Evidence of unusual use of, or other suspicious activity related to, a covered account and
- Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts

Depending on the nature of your business, not all of these categories may be relevant. For example, a financial institution that services only closed-end accounts (e.g., accounts to which customers cannot add additional charges after origination, like a closed-end retail installment sale account) would be unlikely to see “unusual use of, or suspicious activity” in those accounts. On the other hand, open-end accounts, such as credit cards or home-equity lines of credit, are at risk of access by identity thieves, and financial institutions and creditors should develop appropriate policies and procedures for monitoring the activity in those accounts. Some creditors, such as motor vehicle dealers who sell their closed-end installment sale contracts and lease agreements to finance companies, are unlikely to receive notices from customers about identity theft in their accounts, while credit card issuers and cell phone providers may have the opposite experience.

Creditors who routinely obtain consumer reports are accustomed to seeing fraud and active duty alerts. As a general rule, these alerts are red flags that should be included in these creditors' Programs. Presentation of suspicious identification documents, customer addresses that don't appear on any consumer report and fraudulent Social Security numbers also are red flags that should be considered when crafting a Program.

Finally, financial institutions and creditors need not be limited to the categories enumerated in the Red Flags Rule. If other categories exist and are relevant to one's business, they should be considered as well.

Detecting Red Flags

The Red Flags Rule provides that financial institutions and creditors should obtain identifying information about, and verify the identity of, a person opening a covered account. It also recognizes that many institutions already have “know your customer” obligations under the USA PATRIOT Act in place and encourages those institutions to incorporate the policies and procedures of their CIPs into their Identity Theft Prevention Programs, as appropriate. Given the current shortage of regulatory guidance on how to comply with the Red Flags Rule and the relatively detailed CIP procedures in the USA PATRIOT Act, institutions not subject to the USA PATRIOT Act requirements may want to consider using those requirements as a model. To that end, the following discussion looks to the guidance of the USA PATRIOT Act's “know your customer” regulations.

The Red Flags Rule — an overview

Care also should be exercised when granting account access to existing customers. While open-end accounts generally pose a greater identity theft risk, successfully accessing a closed-end account can provide an identity thief with information he or she can use elsewhere to hijack a customer's identity. Many financial institutions and creditors encourage customers to access their accounts via the Internet or telephone and have appropriately integrated automated fraud detection and/or customer identification tools into their account access systems. In addition, many limit access to customer accounts to those customers with a "need to know," both as part of their internal information security programs and to mitigate the potential for employee theft of customer information.

Customer identification information. A Program should specify acceptable identifying information that will be required of each customer applying for a covered account. At a minimum, this should include:

- Name
- Date of birth, for an individual
- Address, which shall be:
 - For an individual, a residential or business street address
 - For an individual who does not have a residential or business street address, an Army Post Office or Fleet Post Office box number or the residential or business street address of next of kin or of another contact individual or
 - For a person other than an individual (such as a corporation, partnership or trust), a principal place of business, local office, or other physical location and
- Identification number, which shall be:
 - For a U.S. person, a taxpayer identification number (such as a Social Security number) or
 - For a non-U.S. person, one or more of the following: a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard

Business and commercial customers should be required to provide a taxpayer identification number ("TIN"). However, in some instances, the business may not have received the TIN yet. In these instances, the Program should require confirmation that the customer filed the TIN application before the account origination process is consummated, as well as a procedure to obtain the TIN from the business customer within a reasonable period of time after the covered account is originated.

Authenticating a customer's identity. A Program should contain procedures for verifying the customer's identity, starting with the identifying information obtained from the customer. These procedures should address customer verification through documents and otherwise.

The Red Flags Rule — an overview

- **Verification through documents.** A Program should contain procedures that set forth documents the financial institution or creditor will accept for identity verification purposes. These documents may include:
 - For an individual, unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport and
 - To the extent persons other than an individual (such as a corporation, partnership or trust) are covered by a Program, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or trust instrument
- **Verification through nondocumentary methods.** Those financial institutions and creditors that originate covered accounts for customers who are not physically present for the transaction, and those who permit customer access to covered accounts remotely (e.g., over the telephone or Internet), should include policies and procedures in their Programs that describe the nondocumentary methods to be used in verifying the customer's identity:
 - These methods may include contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source; checking references with other financial institutions; and obtaining a financial statement
 - The Program also should address situations where:
 - a. the customer is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard
 - b. the documents presented (e.g., an out-of-state driver's license or a foreign passport) are unfamiliar to staff
 - c. the customer is not physically present during the account origination or access process and
 - d. other relevant circumstances where customer identity verification is not possible through use of documentation
- **Additional verification for certain customers.** A Program's policies and procedures should address situations involving business or commercial customers where it may be prudent to obtain information about individuals with authority or control over the financing transaction in order to verify the customer's identity. This typically will include instances where customer identity verification is not possible through use of the financial institution's or creditor's normal verification methods described in its Program.

Responding to Red Flags

Each financial institution and creditor that originates or maintains covered accounts must have reasonable policies and procedures in their Programs to respond to red flags they detect in a manner commensurate with the degree of risk each particular red flag poses — in other words, a risk-based approach to resolving red flags. Additionally, the Red Flags Rule suggests considering aggravating factors that

The Red Flags Rule — an overview

may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to customer account records or notice that a customer has provided information related to his or her covered account to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent Web site.

Many red flags will resolve themselves, either through light inquiry, proprietary or third-party fraud detection and/or customer identification tools, or other preliminary verification process. The more difficult it is to satisfactorily resolve a red flag, the greater the risk it poses and the more concentrated the effort to resolve it should be.

Many Program's policies and procedures for responding to red flags will include an escalation process to involve members of staff better qualified to evaluate the seriousness of a red flag and identify the appropriate response. This approach recognizes the subjective aspects of responding to red flags, as well as the need for greater scrutiny when greater risk is detected. As a practical matter, financial institutions and creditors will want to be sure their staffs are not terminating transactions over easily resolved red flags.

Appropriate responses to red flags run the gamut. In the account origination process, they may include:

- Not continuing the transaction
- Not selling a covered account to a finance company or debt collector
- Notifying law enforcement or
- Determining that no response is warranted under the particular circumstances

Appropriate responses in the covered account maintenance process may include:

- Monitoring covered accounts for evidence of identity theft
- Contacting the customer
- Changing any passwords, security codes or other security devices that permit access to the covered accounts
- Not attempting to collect on a covered account or not selling a covered account to a debt collector
- Notifying law enforcement or
- Determining that no response is warranted under the particular circumstances

Updating the Program

The Red Flags Rule requires financial institutions and creditors to update their Programs (including the red flags they identify as relevant) periodically to reflect

The Red Flags Rule — an overview

changes in risks to customers or to the enterprise's safety and soundness from identity theft. Updates to a financial institution's or creditor's Program should be based on:

- Its experiences with identity theft
- Changes in methods of identity theft
- Changes in methods to detect, prevent and mitigate identity theft
- Changes in the types of accounts it offers or maintains and
- Changes in business arrangements, including mergers, acquisitions, alliances, joint ventures and service provider arrangements

As a practical matter, any identity theft incident a financial institution or creditor experiences will likely trigger an assessment of, and potential update to, its Program. The fact that identity theft occurred could mean there are new red flags that should be added to the Program so the same or similar incident does not occur again. Alternatively, the incident may have presented red flags already identified in the Program that were not detected by staff, indicating a problem with existing policies and procedures or training methods.

The methods used by identity thieves to commit their crimes will evolve over time. This may result from changes in technology, changes in the way customer information is handled, or other relevant changes in how a particular financial institution or creditor operates. Those entities covered by the Red Flags Rule may want to task a particular individual or department, e.g., loss mitigation, with staying apprised of new or modified identity theft methods and update their Programs accordingly.

Many vendors are, or will be, providing automated tools to assist financial institutions and creditors in detecting red flags. At the very least, financial institutions and creditors should periodically evaluate these offerings to determine their value to their particular operations and their economic feasibility.

Different types of accounts require different levels of inquiry in addressing red flags. An auto dealer that does nothing more than originate installment sale and lease transactions that it immediately sells to a finance company is obligated by the Red Flags Rule to authenticate the customer's identity before it closes the transaction and creates the account. However, because it does not maintain the accounts for any appreciable period of time, it will have no existing accounts to monitor for identity theft activity. Even if it held the accounts, to the extent they were closed-end transactions there may be little risk of identity theft during the term of the transaction. On the other hand, a credit card issuer or depository institution will have a greater need to monitor the accounts it services for red flags.

The Red Flags Rule — an overview

Finally, a merger or acquisition of a competitor or a new line of business will require a review of the existing Program or Programs to ensure that policies and procedures are relevant and effective. These corporate transactions generally require a lot of attention to integration, and each company's Program is part of that. Additionally, those entities that outsource activities related to covered accounts to third-party service providers must take some action to ensure the service providers support the entities' compliance obligations.

It's important to remember that there may be other reasons to update a Program. These will become apparent to financial institutions and creditors as they undertake their initial Program development and implementation and over time. The primary objective is to implement a Program that, on the whole, effectively detects, prevents and mitigates identity theft, so any activity that may significantly impact the effectiveness of a Program should trigger a Program review and possible update.

Program administration

The Red Flags Rule requires financial institutions and creditors to manage their Programs and take certain specific actions:

- The initial Program must be approved in writing by the board of directors, an appropriate committee of the board of directors or, if there is no board of directors, a designated senior manager
- That approving party must be involved in the oversight and administration of the Program and must assign specific responsibility for the Program's administration and review the periodic reports required by the Red Flags Rule
- Relevant staff must receive appropriate training, as necessary, to effectively implement the Program and
- Appropriate and effective oversight of relevant service provider arrangements must be exercised

Someone designated by the financial institution's or creditor's board or senior management, as applicable, must prepare at least annual reports evaluating the state of the institution's compliance with its Program. These reports must address material matters related to the Program and can be made at any appropriate time, i.e., financial institutions and creditors need not (and, in some instances, should not) wait a year between reports. For example, it may be sensible to prepare a report after a significant experience with identity theft, even if the prior report was recently submitted.

At a minimum, the periodic reports should evaluate:

- The effectiveness of the Program's policies and procedures in addressing the risk of identity theft in connection with the account origination and maintenance processes
- Arrangements with service providers involved in the account origination or maintenance processes
- Significant incidents involving identity theft and management's response and
- Recommendations for material changes to the Program

Address discrepancies

Included in the publication of the Red Flags Rule were rules implementing two additional FACT Act requirements. One is part of the Red Flags Rule authorization in Section 114 of the FACT Act and requires credit and debit card issuers to assess the validity of notifications of changes of address under certain circumstances. The other implements Section 315 of the FACT Act and provides guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy.

Duties of users regarding address discrepancies

At their core, the rules implementing Section 315 of the FACT Act require a user of a consumer report to develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report. This should occur when the user receives a notice of address discrepancy from the consumer reporting agency from which it requested the consumer report. These policies and procedures must include a requirement that the user furnish a “confirmed” address to the consumer reporting agency from which it receives a notice of address discrepancy in the ordinary course of its reporting, but no later than the reporting period in which the consumer relationship is established.

The requirements are driven by definitions. For example, a “notice of address discrepancy” is defined as “a notice sent to a user by a consumer reporting agency ..., that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency’s file for the consumer.” Consequently, a user who does not provide an address when requesting a consumer report will not (and cannot, by definition) receive a notice of address discrepancy.

The rule contains guidance with respect to what are “reasonable policies and procedures.” For example, these include (a) verifying the information in the consumer report with the consumer or (b) comparing the consumer report information to information (i) the user collects as part of its USA PATRIOT Act CIP, (ii) it maintains in its own files or (iii) it obtains from third-party sources. While there is no express requirement that these policies and procedures be in writing (unlike the Red Flags Rule), there appears to be an implied expectation that they will, e.g., language such as, “The policies and procedures developed ... must provide that the user will furnish the consumer’s address that the user has reasonably confirmed is accurate”

Users also must develop and implement reasonable policies and procedures for furnishing to the consumer reporting agency from which it has received a notice of address discrepancy an accurate address for the consumer that the user has reasonably confirmed. This requirement is triggered when the user (a) can form a reasonable belief that the consumer report relates to the consumer about whom

Address discrepancies

the user requested the report, (b) establishes a continuing relationship with the consumer and (c) regularly and in the ordinary course of business furnishes information to that consumer reporting agency. Definitions are important here as well, i.e., the rule only requires a user to report an accurate address if it regularly furnishes information to the consumer reporting agency from which it receives a notice of address discrepancy. In other words, if the user does not regularly furnish information, or if it receives a notice of address discrepancy from a consumer reporting agency to which it does not regularly furnish information, there is no requirement to furnish an accurate address.

For users that must furnish an accurate address, such accuracy can be confirmed by (a) verifying the address with the consumer, (b) reviewing the user's own records to verify the address of the consumer, (c) verifying the address through third-party sources or (d) using other reasonable means. The rule does not expand on what would be "reasonable," but one could assume that the methods described should be viewed as a floor rather than a ceiling.

Finally, to the extent a user must report an accurate address, its reasonable policies and procedures "must provide" that it will furnish the confirmed address to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which the consumer relationship is established. While this language does not expressly require policies and procedures to be in writing, many users subject to the furnishing requirement will be likely to use writing as a means of proving their compliance with it.

Duties of card issuers regarding changes of address

Section 114 of the FACT Act mandates financial institutions and creditors to develop and implement an Identity Theft Prevention Program. In addition to that substantive requirement, it also mandates debit and credit card issuers to establish and implement reasonable policies and procedures to assess the validity of a consumer cardholder's new address when it receives notification of a change of address, and, within a short period of time afterward (during at least the first 30 days after it receives the change of address notice), it receives a request for an additional or replacement card for the same account.

A card issuer may not issue an additional or replacement card until it validates the consumer cardholder's new address in accordance with its reasonable policies and procedures. These policies and procedures must provide for notifying the cardholder of the request at his or her former address or by whatever means to which the parties have previously agreed. Any written or electronic notice to the cardholder must be clear and conspicuous and separate from other regular correspondence with the cardholder. The rule does not preclude nonwritten validation methods.

Address discrepancies

The issuer also must provide a reasonable means for the cardholder to promptly report incorrect address changes or must otherwise assess the validity of the change of address in accordance with its Identity Theft Prevention Program. Operationally, a card issuer need not wait for a replacement card request; the rule permits a card issuer to validate the new address before it receives a request for an additional or replacement card.

Change of Address

According to the United States Postal Service[®], more than 40 million Americans change their address annually, which creates formidable obstacles in maintaining a high-quality mailing list. To help reduce undeliverable mail pieces before they enter the mail stream, the USPS[®] offers the NCOA^{Link}[®] product. By completing the certification process, companies can obtain a license to use NCOA^{Link} product, which allows them to electronically access information provided by consumers on a USPS change of address form. By having access to current address change information, businesses can continue marketing or otherwise mailing to their current clients.

The NCOA^{Link} service provides updated addresses for individuals, families and businesses. The USPS certifies software used to perform the NCOA^{Link} process, ensuring that the addresses in a provider's database are specifically designed to match the USPS requirements. The software will update old addresses through the information provided by the NCOA^{Link} service.

Financial institutions and creditors have good reason to be concerned about the validity of the information contained in the NCOA^{Link} systems. The NCOA^{Link} systems do not validate the address change information; they merely regurgitate it. Identity thieves have been known to intercept a victim's credit card statement, submit a change of address for the victim to a PO Box or other address the identity thief can access, and request a new card from the card issuer. Once the new card is available, the identity thief can use up the available credit on the card as well as use the information obtained to open additional fraudulent accounts.

Section 114 of the FACT Act addresses the issue of identity thieves gaining access to a consumer's credit or debit card accounts by mandating the rule discussed in this section. It addresses broader identity theft opportunities, i.e., using the information one can obtain by diverting a consumer's mail to create new credit accounts with the new address, by requiring financial institutions and creditors to develop and implement Identity Theft Prevention Programs. Because these Programs must be designed to detect, prevent and mitigate identity theft prevention in the account opening and maintenance processes, financial institutions and creditors may consider implementing policies and procedures for independently validating a customer's change of address received through the NCOA^{Link} process or otherwise.

Common operational challenges

Common operational challenges impacting compliance with the Red Flags Rule

There is a learning curve associated with new compliance obligations, and the Red Flags Rule is no different. Identifying operational compliance issues will be straightforward in some instances and more complex in others, but one can be sure that operational realities will impact compliance efforts. Some additional guidance will likely continue to be disseminated from the federal regulatory agencies with examination authority, most likely through the publication of examination guidelines. For example, on Aug. 11, 2008, The Office of Thrift Supervision (OTS) released clarifying statements regarding examination procedures related to the Red Flags Rule.

Despite the dearth or ambiguity of guidance, certain operational compliance concerns can be anticipated. These include concerns about infrastructure, report management, staff training, referral volumes, customer experience, operational costs, and potential ambiguity in guidance and examinations, to name a few, and all point to the need for clear guidance from regulators. Additionally, the Red Flags Rule's vague enforcement standard — that financial institutions and creditors will be evaluated not on whether their Programs control for any particular red flags, but on the effectiveness of their Programs — may leave even the most credible compliance officers with some doubt about the appropriateness of their programs.

Infrastructure

The Red Flags Rule requires internal oversight at a high level, i.e., by the board (or an appropriate committee of the board) or by a designated senior manager or bank official, as applicable. In any organization, oversight comes at a price, and overseeing the design and implementation of the Red Flags Rule will be no different.

Some organizations are accustomed to exercising oversight authority at a high level. The boards of financial institutions, both large and small, routinely engage in oversight activities, and while additional oversight requirements can create additional burdens, these organizations are likely to adapt fairly easily to the new obligations.

On the other hand, organizations such as auto dealers, wireless providers, retailers and medical providers, etc., may have little experience with the type of oversight contemplated by the Red Flags Rule. In fact, some may have no active infrastructure through which to address either their oversight or design and implementation obligations.

There are also infrastructure concerns that revolve around Program implementation. For many financial institutions, the Red Flags Rule represents nothing more than a codification of their existing fraud prevention efforts. Organizations with CIPs pursuant to the USA PATRIOT Act will meld those programs with their obligations

Common operational challenges

under the CIP. Organizations already subject to the Gramm-Leach-Bliley Act's Information Safeguarding Rule can turn to the design, implementation and oversight process for their respective Information Security Programs as a starting point for Red Flags Rule compliance. However, there will be a significant number of organizations having little experience with designing and implementing a program like that which is required under the Red Flags Rule. These organizations, in particular, will benefit from agency guidance regarding the more practical aspects of the overall compliance process.

Implementation of additional consumer authentication processes, whether internally developed, vendor delivered or a combination of both, will require some level of technical and operational investment and support. As Nov. 1, 2008, approaches and passes, institutions are urged to plan for vendor selection, implementation, training and optimization of embedded processes.

Report management

The Red Flags Rule requires financial institutions and creditors to prepare periodic reports evaluating the organization's compliance with its Identity Theft Prevention Program at least annually. These reports should evaluate the Program's effectiveness, arrangements with service providers, significant identity theft incidents experienced by the organization and recommendations for material changes to the Program.

Any reporting process requires thought and consideration as well as time and labor. A reporting requirement prescribed by regulation imposes additional burdens as organizations speculate about the standard by which their efforts will be judged and struggle to define the standard by which they will judge themselves.

How those subject to the Red Flags Rule will be judged is uncertain. Should the barometer be a smaller incidence of identity theft? If so, how does one define identity theft for evaluation purposes? Should the standard focus on process? Is more process better than less? Is using a checklist for each transaction better than targeting efforts and resources on transactions that contain more apparent risk indicators? There are many questions but not many answers.

Organizations will be looking to their regulating agencies for guidance on what Programs should look like, and many will build Programs to the agencies' expectations. The efficacy of this approach, at least in terms of meeting the objectives of the Red Flags Rule, is questionable at best. But it may be one of the only useful yardsticks against which to measure compliance efforts.

In choosing external vendor products and services, many have performance reporting available, which may serve to meet much of the overall reporting requirements of the Red Flags Rule. In fact, such reporting should provide both internal and external examiners with a level of confidence in the performance of selected tools as well as a means of determining any necessary alterations to the process over time.

Common operational challenges

Staff training

The Red Flags Rule requires that relevant staff receive appropriate training, as necessary, to effectively implement the Program. Focus should be placed on those staff directly involved in the account origination customer identity verification process, as well as those who respond to customer inquiries and those who have the type of access to account information such that they could recognize potential red flags in account activity.

Training can take many forms, from lectures to PowerPoint® presentations to videos to information and assessment programs. Each organization will determine the best approach for its specific circumstances, but at a minimum, training should consist of an explanation of the red flags the organization identifies in its Program, how to detect the red flags, and what to do if any particular red flags are detected. Relevant staff should be well informed of what is expected of them, and be provided with appropriate tools to meet their obligations.

Consider, for example, the value of using Customer Identification Checklists in the account origination process. While perhaps appealing because it provides consistency and means of measuring staff performance (and by extension, the suitability of the organization's training efforts), process-laden methods can stifle the user's ability to see that which it may not expect in a transaction. Staff may tend to "play to the checklist" and miss potential red flags they don't specifically seek. On the other hand, they are unlikely to miss the red flags you've included in your Program.

Some may favor a risk-based approach, where automated decisions can be made about the likelihood of identity theft early in a transaction and more rigorous (and expensive) verification efforts can be focused on those transactions with higher risk scores. This approach helps prioritize resources but doesn't necessarily provide a quantifiable means of evaluating staff performance or enterprise training methods.

The value of a risk-based approach with consistent decisioning policies lies in the consistency itself. Rather than relying on the subjectivity of manual staff review, institutions may adopt a process that minimizes the potential for varied outcomes across the same set of conditions.

Referral volumes

One of the more significant operational concerns is with referral volumes, i.e., the potential that the account origination or maintenance process will get bogged down due to a significant number of red flags detected. These concerns are not without merit. Financial institutions and creditors are likely to err on the side of caution, and, as a result, many transactions may be subject to greater customer identification scrutiny than is necessary.

Common operational challenges

Organizations may be able to control referral volumes through the use of automated tools that evaluate the level of identity theft risk in a given transaction. For example, customers with a low-risk authentication score can be moved quickly through the account origination process absent any additional red flags detected in the ordinary course of the application or transaction. In fact, using such tools may allow organizations to speed up the origination process for these customers and identify and focus resources on those transactions that pose the greatest potential for identity theft.

A risk-based approach to Red Flags compliance affords an institution the ability to reconcile the majority of detected Red Flag conditions efficiently, consistently and with minimal consumer impact. Detection of Red Flag conditions is literally only half the battle. In fact, responding to those Red Flag conditions is a substantial problem to solve for most institutions. A response policy that incorporates scoring, alternate data sources and flexible decisioning can reduce the vast majority of referrals to real-time approvals without staff intervention or customer hardship. Experian's risk-based approach will be discussed in more detail later in this document.

Customer experience

Financial institutions and creditors may have legitimate concerns about the effect of their Program on the customer experience. It is certainly possible that as a result of the Red Flags Rule, some significant number of customers will find themselves subject to more rigorous scrutiny about their identity. Organizations will want to ensure that such scrutiny is effective while at the same time limiting its invasiveness. As a practical matter, organizations will want to apply the stricter scrutiny to the fewest number of customers necessary, and finding that dividing line may be tricky.

Implicit in the concerns about referral volumes above are also open questions about the customer experience. Additional identity verification efforts, if implemented too bluntly, are likely to drive some legitimate customers away. On the other hand, some identity thieves may walk away as well. For knowledgeable and comparison-shopping customers, "customer experience" may be the tipping point for a consumer when choosing one service provider over another.

Operational costs

All regulatory burdens come with operational costs, and the Red Flags Rule is no different. In fact, every challenge discussed in this section involves a cost, both in money and time. For example, someone will need to take ownership of the Program, staff will need to be trained and someone will have to train them, reports will need to be prepared, and service providers will need to be evaluated. Referral volumes will need to be managed, and marketing efforts will be exerted to tout the value of an organization's identity theft prevention policies.

Common operational challenges

Large financial institutions and creditors with multiple lines of business may be able to take advantage of some economies of scale, but they still will face significant cost, particularly in the development and implementation of their Programs. Smaller financial institutions and creditors, especially those lacking existing infrastructure and experience with this kind of regulatory compliance, may expend fewer actual dollars but a greater percentage of their revenue. What remains to be seen is whether the efforts undertaken to comply with the Red Flags Rule will produce the desired result — namely, to detect, prevent and mitigate identity theft.

Potential ambiguity in guidance and examinations

Finally, financial institutions and creditors are faced with uncertainty about how they will be evaluated and whether evaluation will be consistent with any yet-to-be-published regulatory advice. As indicated above, organizations will be looking to their functional regulators for guidance on how they should be complying with the Red Flags Rule. Perhaps more importantly, they will be looking for consistency in the compliance expectations of those regulators and the standards applied to evaluating the effectiveness of a given Program.

The OTS released information on its Red Flags Rule examination guidelines on Aug. 11, 2008. The examination guidelines are a joint agency effort, i.e., one can assume the separate pronouncements by the other federal functional banking regulators will be substantively similar. Some highlights of the OTS examination guidelines include the following:

- The examiner will verify that the financial institution periodically identifies covered accounts it offers or maintains.
- The examiner will review examination findings in other areas (e.g. Bank Secrecy Act, Customer Identification Program and Customer Information Security Program) to determine whether there are deficiencies that adversely affect the financial institution's ability to comply with the Identity Theft Red Flags Rules.
- The examiner will review any reports, such as audit reports and annual reports prepared by staff for the board of directors (or an appropriate committee thereof or a designated senior management employee) on compliance with the Red Flag Rules. Determine whether management adequately addressed any deficiencies.
- The examiner will verify that the financial institution has developed and implemented a comprehensive written Program, designed to detect, prevent, and mitigate identity theft. The Program must be appropriate to the size and complexity of the financial institution and the nature and scope of its activities.
- The examiner will verify that the financial institution trains appropriate staff to effectively implement and administer the Program.
- The examiner will determine whether the financial institution exercises appropriate and effective oversight of service providers that perform activities related to covered accounts.

Common operational challenges

Conclusion: On the basis of examination procedures completed, the examiner will form a conclusion about whether the financial institution has developed and implemented an effective, comprehensive written Program designed to detect, prevent and mitigate identity theft.

Users of consumer reports must develop reasonable policies and procedures to respond to a notice of address discrepancy they receive from a consumer reporting agency. The OTS has announced five examination steps for this requirement:

- Does the institution recognize the address discrepancy?
- Does it confirm that it relates to the consumer?
- Does it furnish the correct address for the consumer to the credit reporting agency?
- Does it report during the appropriate reporting period? and
- Perform sampling, if needed.

The user may reasonably confirm an address is accurate by:

- Verifying the address with the consumer about whom it has requested the report
- Reviewing its own records to verify the consumer's address
- Verifying the address through third-party sources
- Using other reasonable means

(Source: Office of Thrift Supervision Presentation of Identity Theft Rules and Guidelines, Aug. 11, 2008)' the source refers to all information related above.

Significantly, the OTS noted in its Aug. 11 release that compliance with the Red Flags Rule is not necessarily a new regulatory framework, but an enhancement of existing programs, e.g., Information Security Programs required by the Gramm-Leach-Bliley Act or CIPs required by the USA PATRIOT Act. Many financial institutions and creditors already control for identity theft. For them, compliance will consist primarily of memorializing processes already in place into a written Program. For others, compliance will require more effort. In either case, the OTS examination guidelines provide a glimpse into the expectations of those who will judge the final product and a foundation for building a compliant Program.

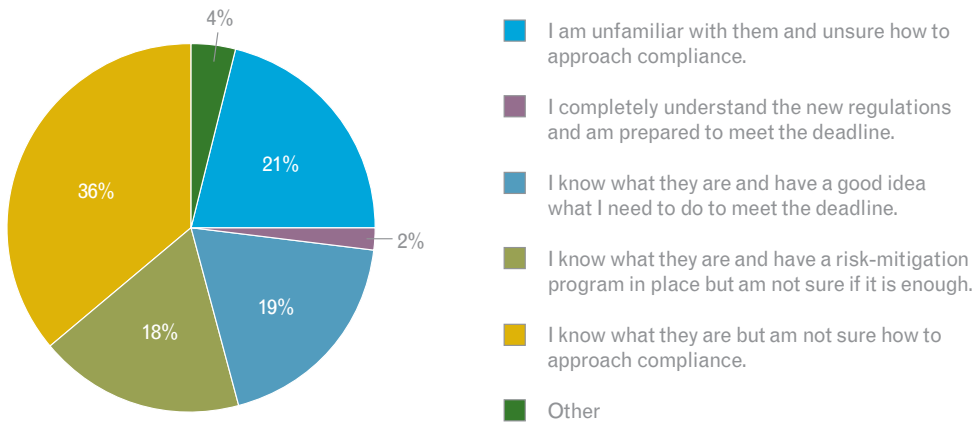
Current market compliance

Current market compliance with the Red Flags Rule

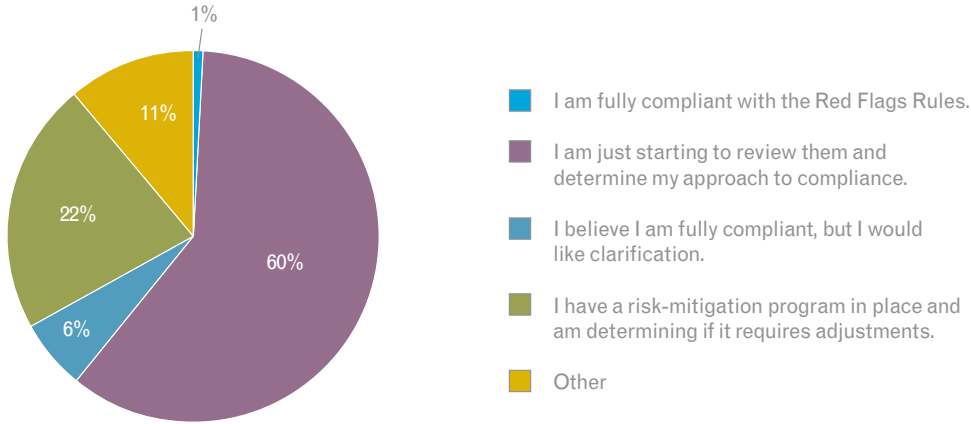
Many surveys abound related to the current market adoption of Red Flag-compliant Identity Theft Prevention Programs. While results may vary, the trend across all surveys indicates that many financial institutions and creditors will not be in compliance with the Red Flags Rule by the Nov. 1, 2008 mandatory compliance date.

Experian conducted a Red Flags Webinar on Feb. 12, 2008, that was attended by more than 850 industry representatives. Real-time surveys were conducted during the session, and the following distribution of both level of understanding and current status are displayed below:

Red Flags Rule understanding

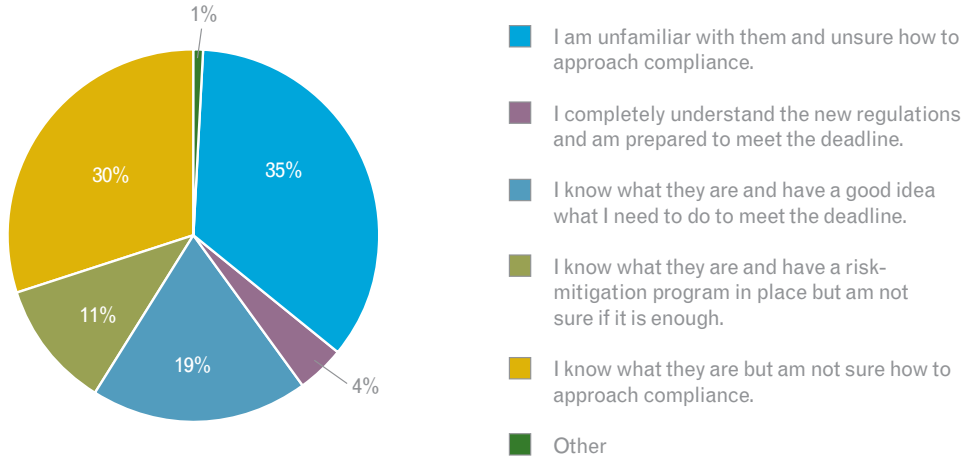


Red Flags Rule status



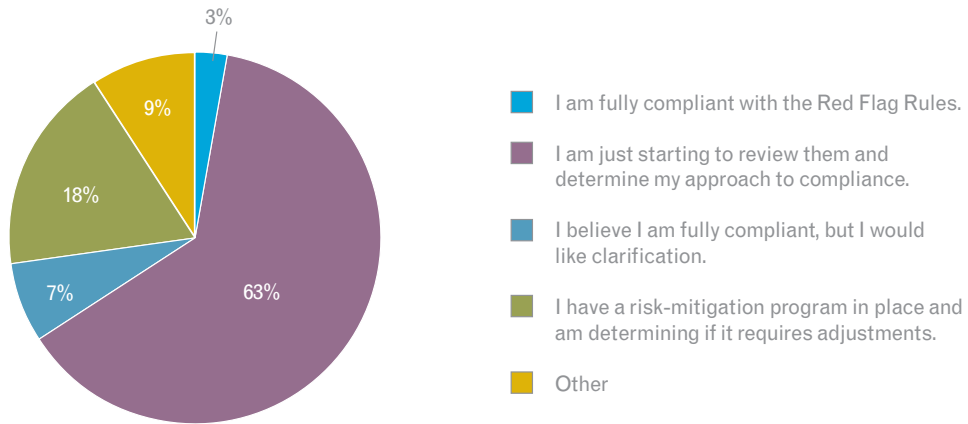
Between May 1, 2008 and July 22, 2008, an additional 74 institution representatives have accessed Experian's Red Flag Webinar. The same survey questions regarding understanding of the Rules and Program status were presented, and the results are displayed below:

Red Flags Rule understanding



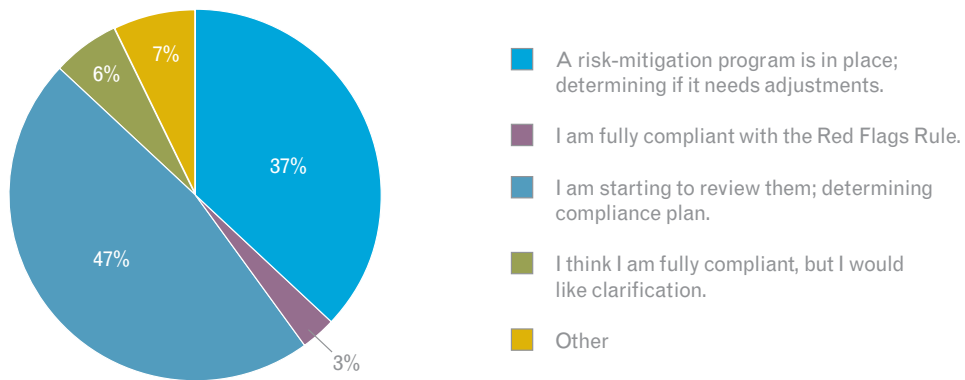
Current market compliance

Red Flags Rule status



Experian launched a micro site dedicated to Red Flags in July 2008. Below is a representation of the current status of micro site registrants (numbering 90 as of Aug. 1, 2008):

Red Flags program status



Regardless of which market survey referenced, there remains little doubt that the level of Red Flags Rule understanding and compliance readiness is widely disparate at a point in time less than four months from the Nov. 1, 2008, compliance deadline.

A risk-based approach to compliance

A risk-based approach to compliance

The ever-changing nature of identity theft practices makes a risk-based and flexible approach to combating it critical. Identity thieves constantly are looking for new methods and targets, and this alone requires financial institutions and creditors to employ dynamic fraud detection techniques and tools. A risk-based approach to managing identity theft potential allows financial institutions and creditors to focus on those areas of operations that pose the greatest danger to themselves and their customers.

Financial institutions and creditors have long had incentives to combat fraud. Many, if not most, already possess sophisticated and rigorous antifraud programs that excel at preventing or mitigating identity theft. Undoubtedly, these efforts focus on operational areas that pose the greatest dangers. Given that financial services organizations can be complex businesses, it is no surprise that the effectiveness of the systems and processes employed to combat identity theft constantly is reviewed. Such review policies indicate that these institutions understand that the identity theft prevention tools that work today will be obsolete tomorrow.

Risk-based compliance gives financial institutions and creditors wide latitude in how they conduct their business, allowing them to focus resources on evaluating the likelihood and severity of identity theft and implementing appropriate detection tools and safeguards. A true risk-based approach will target the operational areas most likely to appeal to fraudsters and identity thieves and apply the most effective controls for the financial institution's or creditor's unique situation.

There are a myriad of vendors offering fraud detection and identity verification tools that can be included in a risk-based Identity Theft Prevention Program to the extent their use is operationally and economically justifiable under the circumstances. Financial institutions and creditors adopting a risk-based approach to the Red Flags Rule should include in their Programs provisions for assessing the value and effectiveness of such tools from time to time as their operations and economics evolve. In particular, financial institutions and creditors should take into account the cost and transaction time savings to be gained from using tools that can assign an "identity theft risk score" to customers, i.e., transactions involving customers with lower-risk scores will not need the added level of identity verification that will be applied to higher-risk customers.

Rather than implementing a "rules-based" 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 Flag 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 effective fraud

A risk-based approach to compliance

prediction models in combination with detailed consumer authentication conditions (such as address mismatches or Social Security number inconsistencies).

A risk-based fraud detection system 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 Rules in the published guidelines are not “silver bullets” that ensure 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 Flag 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 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 increasingly competitive marketplace, “consumer experience” has become a primary focus for many businesses. A 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 latter category — processes are in place for identity theft protection, but a thorough review is needed to ensure complete compliance. This presents a unique opportunity 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 to best assist in achieving compliance.

A risk-based approach to compliance

Key elements of a robust risk-based Identity Theft Prevention Program

Element	Description	Value
Broad-reaching and accurately reported data sources	Data sources spanning multiple public record and/or consumer credit information.	Provides a far-reaching and comprehensive opportunity to positively verify consumer identity elements such as name, address, Social Security number, date of birth and phone.
Targeted analytics	Scores designed to consistently reflect overall confidence in consumer authentication as well as fraud risk associated with identity theft, synthetic identities and first-party fraud.	<p>Allows institutions to establish consistent and objective score-driven policies to reconcile single or multiple Red Flag conditions.</p> <p>Reduce false positives associated with a binary rules method of identity theft risk assessment and segmentation.</p> <p>Provides internal and external examiners with a measurable tool for incorporation into both written and operational Programs.</p>
Detailed and summary-level consumer authentication results	Consumer authentication outcomes that portray the level of verification achieved across identity elements such as name, address, Social Security number, date of birth and phone. Such outcomes should include summary-level codes as well as detailed information obtained via leveraged data sources such as previous addresses, alternate consumers and risk conditions related to specific identity elements.	<p>Delivers a breadth of information to allow positive reconciliation of Red Flag conditions.</p> <p>Specific results can be used in manual or automated decisioning policies as well as scoring models.</p>
Flexibly defined decisioning strategies and link analysis	Data and operationally driven policies that can be applied to the gathering, authentication, and level of acceptance or denial of consumer identity information.	Decisioning strategies afford an institution the ability to employ consistent policies for detecting Red Flag conditions, reconciling those conditions that can be and ultimately determining the response to consumer authentication results — whether it be acceptance or denial of business.

Experian's role in Red Flags Rule compliance

Experian's role in Red Flags Rule compliance

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 Flag–relevant products such as Precise ID,SM clients are notified of consumer alerts, victim statements and freezes, and suspicious personal identifying information, including 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 Flag–relevant products and services that combine:

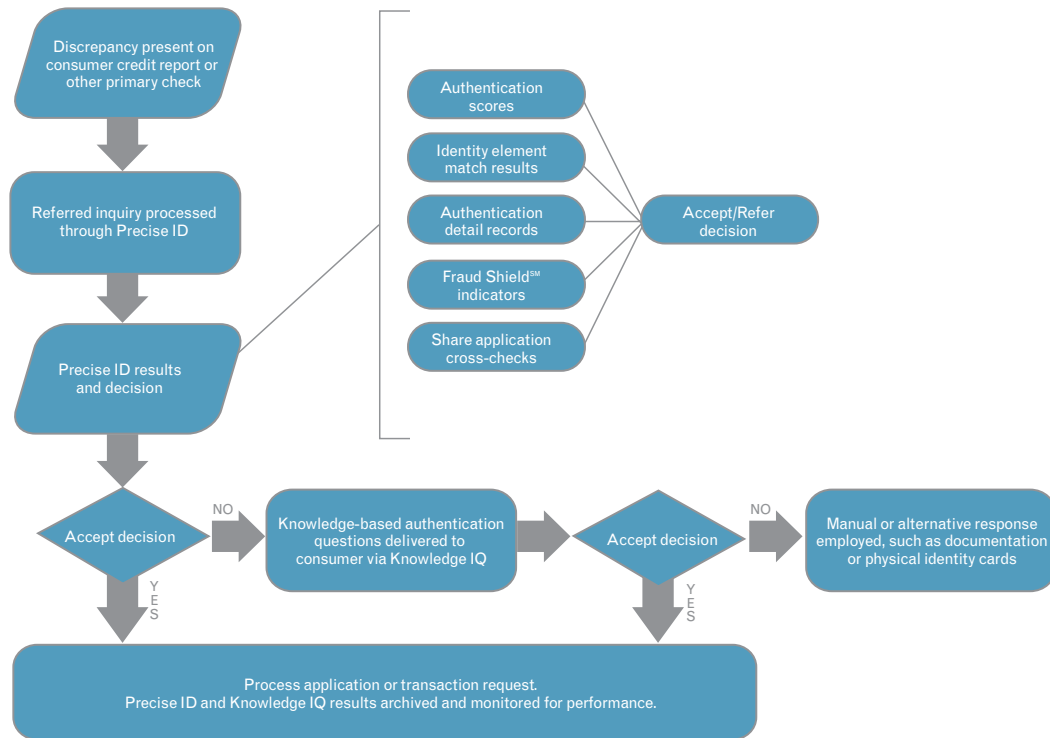
- Consumer credit and noncredit data assets
- Detailed consumer identity information
- Flexible delivery options
- Targeted identity theft and consumer authentication scoring models
- Custom and best-practice decisioning
- Knowledge-based authentication (interactive consumer question-and-answer sessions)
- 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.

Experian's role in Red Flags Rule compliance

Sample employment of Precise ID and Knowledge IQSM in consumer authentication

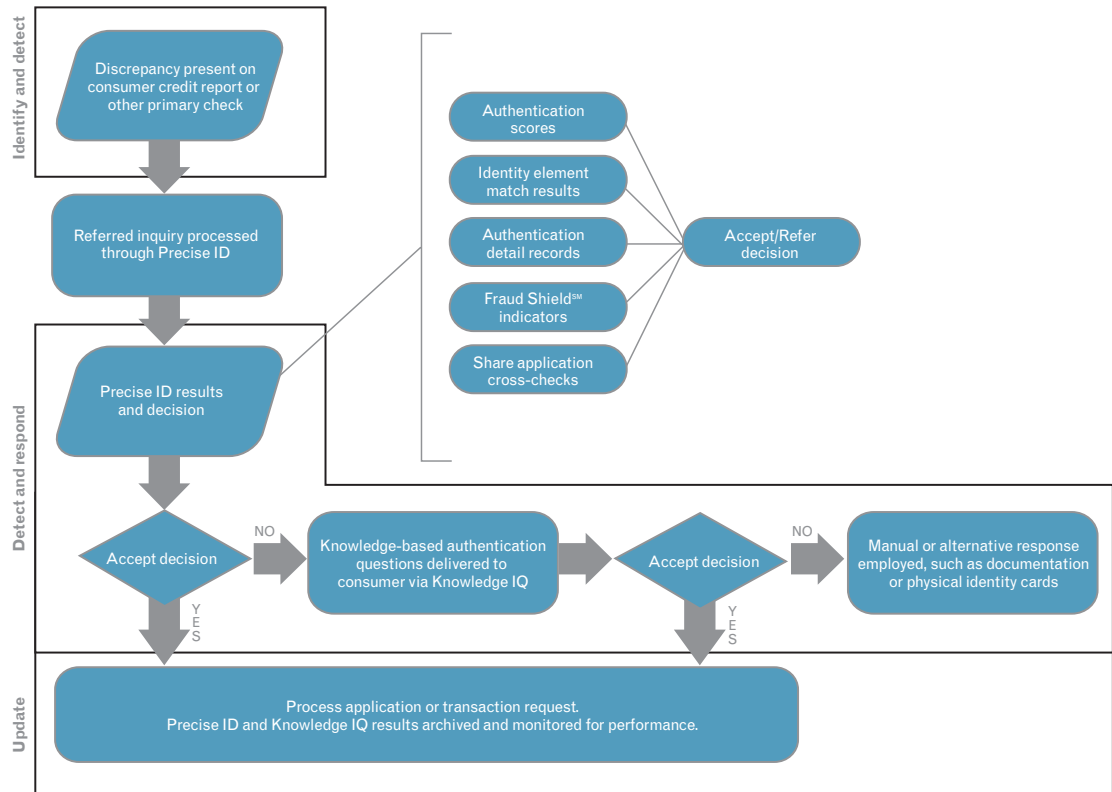


As stated earlier in this paper, a compliant Program must contain reasonable policies and procedures to address four mandatory elements. These are:

- **Identifying** red flags applicable to covered accounts, and incorporating them into the Program
- **Detecting** and evaluating the red flags included in the Program
- **Responding** to the red flags detected in a manner that is appropriate to the degree of risk they pose and
- **Updating** the Program to address changes in the risks to customers and to the financial institution's or creditor's safety and soundness from identity theft

In overlaying these four mandatory elements on Experian's sample employment of Precise ID and Knowledge IQ, one can see the comprehensive inclusion of all of these requirements within a single operational process:

Experian's role in Red Flags Rule compliance



Experian's Precise ID platform provides institutions with a consistent method to:

- Identify and detect Red Flag conditions via:
 - Summary and detailed consumer authentication results (both positive and negative) associated with name, address, Social Security number, date of birth and phone number
 - Authentication scores
 - Additional high-risk conditions including, but not limited to:
 - Deceased Social Security numbers
 - Inconsistent use of identity elements across multiple inquiries or applications
 - High-risk address types or known fraud addresses
 - Credit profile freezes, victim statements or active duty alerts
 - Inconsistent establishment of Social Security number or credit history as related to date of birth
 - Multiple consumers associated or more closely linked with single identity elements such as Social Security number, address and telephone

Experian's role in Red Flags Rule compliance

- Respond to Red Flag detection via:
 - Consumer authentication and identity theft scoring
 - Potential fraud type categorization and score factor codes
 - Positive or negative identity element verification results
 - Presence or absence of high-risk conditions
 - Automated decisioning
 - Knowledge-based authentication session results (if applicable)
- Update Red Flag Identity Theft Prevention Programs via:
 - Performance monitoring
 - Archived reports
 - Consultation with Experian support team

The key to an effective and optimal risk-based Program lies in the breadth and variance of elements available for use in decisioning. A Program with limited data sources, results and scoring capability is inherently bounded by those elements when determining decisioning thresholds and criteria. A Program and risk-based platform that incorporates multiple data sources, aggregate and sub-level scoring, and detailed verification results and record information will, by nature, provide institutions with more options and “dials to turn” as they strike the critical triangular balance of:

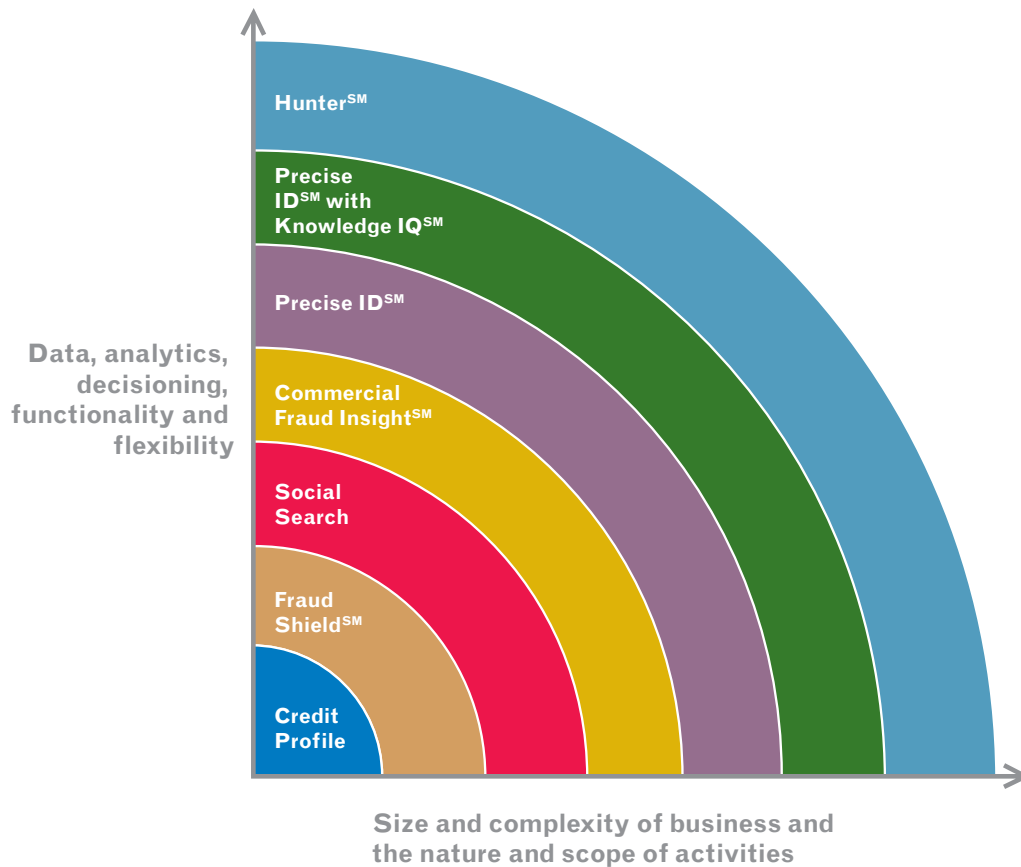
- Compliance
- Fraud detection and
- Application and transaction approval rates

Experian offers a series of Red Flag–relevant products and services that combine:

- Credit and/or noncredit data
- Analytics — authentication and fraud detection
- Decisioning — custom or best practice
- Flexible delivery options — Web user interface, XML, real-time, batch

Depending on the size and complexity of an institution's business and the risk its related activities pose to both consumers and the institution itself, Experian offers products that are commensurate with operational requirements:

Experian's role in Red Flags Rule compliance



Credit Profile Report — Generated by Experian's File OneSM system, the report provides an exhaustive search of an applicant's credit history and monitors, evaluates and makes decisions based on changes in the customer profile:

- More than 215 million credit-active consumers via File One
- Consumer statements
- Credit freeze
- FACTA address discrepancy
- Social Security number issuance
- Tradeline history and activity

Fraud ShieldSM — Through a series of checks, searches and counters, Fraud ShieldSM returns indicators that provide specific high-risk descriptions and discrepancies related to identity elements:

- Twenty-seven high-risk warnings across address, Social Security number and credit establishment

Experian's role in Red Flags Rule compliance

- Discrepancies in age related to Social Security number and trades and identity elements
- Victim statements

Note: The majority of Fraud Shield indicators can map directly to the illustrative Red Flag rules noted in the guidance.

Social Search — This tool instantly matches and retrieves the latest consumer identifying information reported on the input Social Security number from the File One database:

- Multiple Social Security numbers per search
- Multiple consumers per Social Security number
- Multiple addresses per consumer
- Fair Credit Reporting Act (FCRA) and non-FCRA versions
- Additional demographics
- First and last reported dates

Commercial Fraud InsightSM — This product draws on multiple databases to provide a comprehensive commercial fraud and authentication tool that quickly analyzes data on business and business principal information. Through a single inquiry, Commercial Fraud InsightSM:

- Validates and verifies business and guarantor application data
- Provides high-level alerts and detailed information from multiple sources
- Identifies previously submitted application elements

Precise IDSM — This comprehensive fraud prevention and detection platform combines detailed consumer authentication results with powerful analytics and customizable decisioning:

- Credit and noncredit data sources and product versions
- Detailed consumer identity checking results and records
- Shared application data and checks
- Targeted models and decisioning
- National Fraud DatabaseSM

Knowledge IQSM — This product leverages Precise ID comprehensive data assets, analytics and decisioning to deliver interactive challenge and response questions to consumers for an added level of confidence and authentication:

- Knowledge-based (out-of-wallet) authentication
- Credit and noncredit versions
- Flexibly weighted and progressive questioning
- Multiple delivery options
- Performance monitoring

Experian's role in Red Flags Rule compliance

HunterSM — Logic checks determine fundamental inconsistencies with application information while utilizing cross-checking and link analysis against multisource data:

- Shared application anomalies
- Identity element misuse or discrepancies
- Consortium- and client-based
- Custom and best-practice rules
- Case management

The following matrix suggests potential mapping of Experian products to various illustrative Red Flag rules:

Rule/Sub-Rule	Fraud Shield SM	Precise ID SM for Account Opening	Precise ID SM for Identity Screening	Hunter SM	Knowledge IQ SM	File One SM Credit Profile	Social Search	Commercial Fraud Insight SM
Category — Alerts, Notifications or Warnings from a Consumer Reporting Agency								
A fraud or active-duty alert is included with a consumer report.	•	•				•	•	
A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.		•	•	•		•	•	
A consumer reporting agency provides a notice of address discrepancy.	•	•	•	•		•	•	
A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:								
a. A recent and significant increase in the volume of inquiries;	•	•				•	•	
b. An unusual number of recently established credit relationships;	•					•		
c. A material change in the use of credit, especially with respect to recently established credit relationships; or						•		
d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.						•		
Category — Suspicious Personal Identifying Information								
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; or	•	•	•			•	•	•
b. The Social Security number has not been issued or is listed on the Social Security Administration's Death Master File.	•	•	•			•	•	•
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 correlation between the Social Security number range and date of birth.	•	•	•	•		•	•	•
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. For example:								
a. The address on an application is the same as the address provided on a fraudulent application; or	•	•	•	•		•	•	•
b. The phone number on an application is the same as the number provided on a fraudulent application.		•		•				
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. For example:								
a. The address on an application is fictitious, a mail drop or prison; or	•	•	•			•	•	•
b. The phone number is invalid or is associated with a pager or answering service.		•	•					•

The chart above represents potential mapping of specific product capabilities for use in your overall Identity Theft Program and should be used only as a reference in developing your self-certified program. For a complete list of Rules, see the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transaction Act of 2003.

Experian's role in Red Flags Rule compliance

Rule/Sub-Rule	Fraud Shield SM	Precise ID SM for Account Opening	Precise ID SM for Identity Screening	Hunter SM	Knowledge IQ SM	File One SM Credit Profile	Social Search	Commercial Fraud Insight SM
Category — Suspicious Personal Identifying Information								
The Social Security number provided is the same as that submitted by other persons opening an account or other customers.	●	●	●	●		●	●	●
The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or other customers.	●	●	●	●		●	●	●
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.								
Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.	●	●	●	●		●	●	●
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.					●			
Category — Unusual Use of, or Suspicious Activity Related to, the Covered Account								
Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional or replacement cards or a cell phone or for the addition of authorized users on the account.		●	●			●		
A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:								
a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or								
b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.		●				●		
A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:								
a. Nonpayment when there is no history of late or missed payments;						●		
b. A material increase in the use of available credit;						●		
c. A material change in purchasing or spending patterns;								
d. A material change in electronic fund transfer patterns in connection with a deposit account; or								
e. A material change in telephone call patterns in connection with a cellular phone account.								
Category — 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 or Creditor								
The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority or any other person that it has opened a fraudulent account for a person engaged in identity theft.	●	●	●			●	●	

The chart above represents potential mapping of specific product capabilities for use in your overall Identity Theft Program and should be used only as a reference in developing your self-certified program. For a complete list of Rules, see the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transaction Act of 2003.

Sample policies and procedures

Sample policies and procedures

This information is provided for informational purposes only and does not constitute legal advice or any endorsement by Hudson Cook LLP or Experian of any named products or services. All questions regarding compliance with the laws and regulations discussed here should be directed to competent legal counsel.

The following sample policies and procedures are for illustrative purposes only. Each organization must fully define and develop their own written Identity Theft Prevention Program.

Statement of objectives

Definitions

- Company: _____
- Account: [Organization-specific description of the Company's covered accounts under the Red Flags Rule]
- Staff: All personnel (whether employees or contractors) who are involved in the collection, use and maintenance of information relating to the Company's Accounts
- Service Providers: Service Providers include any person or organization providing services to the Company that may have access to Accounts or have access to the information contained in Accounts

Program administration

In general

- **Development of the Program:** [The Board of Directors] [The Audit Committee] [Specified individual] is responsible for overseeing the development, implementation and administration of this Program. [The Board of Directors] [The Audit Committee] [Specified individual] must approve this Program and any updates to this Program. Such approval(s) shall be in writing and shall be maintained with this Program.
- **Implementation responsibility:** [The Board of Directors] [The Audit Committee] [Specified individual] may appoint a Program Manager to manage the day-to-day responsibility for developing, implementing and administering this Program. In the absence of such appointment, [The Board of Directors] [The Audit Committee] [Specified individual] shall perform the duties of the Program Manager provided, however, that [The Board of Directors] [The Audit Committee] [Specified individual] may assign specific tasks to designated employees.

Sample policies and procedures

- **Training:** The Program Manager shall ensure that all Staff receive appropriate training with regard to their duties and obligations under this Program:
 - The Program Manager will prepare or approve a training program designed to educate Staff about their duties and obligations under this Program.
 - The first training will be provided to all Staff prior to Nov. 1, 2008.
 - Training for Staff hired or engaged on or after Nov. 1, 2008, shall take place as part of the new-hire/contractor orientation process.
 - All Staff will receive refresher training each time this Program is updated. In the event this Program is not updated during any particular 12-month period, all Staff will receive refresher training prior to the expiration of such 12-month period.
- **Service Providers:** On occasion, the Company may contract with third parties for various tasks associates with Accounts or the information contained in such accounts. The Program Manager will oversee all Service Providers:
 - All Service Providers will be contractually obligated to maintain appropriate safeguards that comply with federal regulations to protect the confidentiality, security and integrity of Account information.
 - The Program Manager will conduct due diligence, as he or she deems appropriate, to develop a reasonable belief that a Service Provider can appropriately safeguard Account information.
 - Service Providers who are involved in the Account origination and/or maintenance process will contractually agree to comply with this Program. Alternatively, the Program Manager may, on a case-by-case basis, require Service Providers to otherwise contractually agree to those specific actions that the Program Manager, in his or her discretion, determines are consistent with the objectives of this Program.

Developing the Program

- The Program Manager will develop this Program using policies and procedures reasonably believed to be effective at identifying Red Flags associated with a reasonably foreseeable risk of identity theft
- This Program will include existing Red Flags that the Program Manager has determined are an effective means of detecting identity theft
- To the extent the Company has implemented, or in the future implements, a CIP in accordance with Section 326 of the USA PATRIOT Act, this Program should be coordinated with such CIP

Maintaining and updating the Program

- *Program review:* The Program Manager will review this Program after any identity theft incident the Company experiences and at least once every 12 months.

Sample policies and procedures

- **Update criteria.** The Program Manager will update this Program after such review, if necessary, to reflect changes in risks to customers and to the safety and soundness of the Company from identity theft. In recommending updates to this Program, the Program Manager will consider factors such as:
 - The Company's experiences with identity theft
 - Changes in methods of identity theft
 - Changes in methods to detect, prevent and mitigate identity theft
 - Changes in the types of Accounts the Company offers or maintains and
 - Changes in the Company's business arrangements, including mergers, acquisitions, alliances, joint ventures and Service Provider arrangements
- **Reports.** The Program Manager shall prepare a report documenting the state of the Company's compliance with this Program and recommending any changes to the Program that are in the opinion of the Program Manager necessary after any identity theft incident but in no case less than at least every 12 months:
 - Such report will be submitted to [The Board of Directors] [The Audit Committee] [Specified individual] for review and comment
 - The report will address material matters related to the Program and evaluate:
 - The effectiveness of the Program in addressing the risk of identity theft in connection with the opening of Accounts and with respect to existing Accounts
 - Service Provider arrangements, including the identity and obligations of each
 - Significant incidents of identity theft experienced by the Company since the prior report and the Company's response and
 - Recommendations for material changes to the Program
 - [The Board of Directors] [The Audit Committee] [Specified individual] will approve all changes made to this Program
 - The Program Manager will implement any changes to the Program as directed by [The Board of Directors] [The Audit Committee] [Specified individual]
- **Documentation:** All updates to this Program and their associated approvals shall be documented and maintained for at least _____ years
- **Risk assessment**
 - The Program Manager will identify the Accounts subject to this Program and conduct an assessment of the Company's risks relative to an identity theft incident relating to such Accounts.
 - The risk assessment will consist of a review of the Company's current policies and procedures directed at detecting and preventing identity theft and the Red Flags associated with such policies and procedures.
 - The Program Manager will evaluate the effectiveness of the Company's current policies and procedures with respect to detecting, preventing and mitigating identity theft relating to Accounts and prepare a written report documenting such policies and procedures and his or her conclusions regarding their effectiveness. Such report shall be maintained with this Program.

Sample policies and procedures

Identifying Red Flags

Policies and procedures for identifying Red Flags

- **Red Flags list:** The Red Flags that are part of this Program are listed in Exhibit 1. The Program Manager will update such list from time to time as necessary to keep this Program current.
- **Considerations for identifying Red Flags:** In identifying relevant Red Flags associated with the origination or maintenance of the Company's Accounts, the Program Manager will consider:
 - The methods employed by the Company to open Accounts — for example, in person, via the Internet, over the phone, etc.
 - The methods through which the Company allows access to Accounts, either by customers, employees, contractors or others.
 - The Company's previous experiences with identity theft.
- **Sources of Red Flags:** The Program Manager will identify Red Flags to be part of this Program from the following sources:
 - The Company's existing policies and procedures
 - Incidences of identity theft the Company has experienced
 - New methods of identity theft arising from changes in identity theft risks
 - Guidance from supervisory agencies
- **Categories of Red Flags:** The Program Manager will identify Red Flags to be part of this Program from the following categories:
 - Alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services. These Red Flags include:
 - A fraud or active duty alert included with a consumer report
 - A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report
 - A consumer reporting agency provides a notice of address discrepancy
 - A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 1. A recent and significant increase in the volume of inquiries
 2. An unusual number of recently established credit relationships
 3. A material change in the use of credit, especially with respect to recently established credit relationships — for example, significant recent use of existing credit accounts that have otherwise been relatively inactive or only moderately active or
 4. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor

Sample policies and procedures

- Presentation of suspicious documents. These Red Flags include:
 - Documents provided for identification appear to have been altered or forged — for example, fraudulent driver's licenses or passports or foreign or any other identification documents that may be unfamiliar
 - The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification
 - Other information on the identification is not consistent with information provided by the person presenting the identification — for example, the information encoded on the driver's license bar code is inconsistent with the information printed on the license
 - An application appears to have been altered or forged or gives the appearance of having been destroyed and reassembled
- Presentation of suspicious personal identifying information. These Red Flags include:
 - Personal identifying information provided by the customer is inconsistent when compared against external information sources used by the Company for credit, fraud detection or other purposes. For example:
 1. The address provided by the customer in the application does not match any address in the customer's consumer report or
 2. The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File
 - The customer presents conflicting personal identifying information — for example, there is a lack of correlation between the SSN range and date of birth or the SSN geocode and the customer's address at the time the SSN was issued.
 - Personal identifying information provided is associated with known fraudulent activity, as indicated by internal or third-party sources used by the Company. For example:
 1. The address on an application is the same as the address provided on a fraudulent application or
 2. The phone number on an application is the same as the number provided on a fraudulent application
 - Personal identifying information provided is of a type commonly associated with fraudulent activity, as indicated by internal or third-party sources used by the Company. For example:
 1. The address on an application is fictitious, a mail drop or a prison or
 2. The phone number is invalid or is associated with a pager or answering service
 - The SSN provided is the same as that submitted by other persons opening an Account or other customers.
 - The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons submitting credit applications.

Sample policies and procedures

- The customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that the Company has on file. For example, a “repeat” customer provides personal identifying information such as an SSN that is inconsistent with the information contained in the Company’s files.
- Unusual use of, or suspicious activity related to, the Account. These Red Flags include:
 - Shortly following the notice of a change of address for an Account, the Company receives a request for a new, additional or replacement [card or cell phone] or for the addition of authorized users on the Account.
 - A new revolving Account is used in a manner commonly associated with known fraud patterns. For example:
 1. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry) or
 2. The customer fails to make the first payment or makes an initial payment but no subsequent payments
 - A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 1. Nonpayment when there is no history of late or missed payments
 2. A material increase in the use of available credit
 3. A material change in purchasing or spending patterns
 4. A material change in electronic fund transfer patterns in connection with a deposit account or
 5. A material change in telephone call patterns in connection with a cell phone account
 - An 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).
 - Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer’s Account.
 - The Company is notified that the customer is not receiving paper Account statements.
 - The Company is notified of unauthorized charges or transactions in connection with a customer’s Account.
- Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with Accounts maintained by the Company. These Red Flags include:
 - Receipt of a notice from a customer, a victim of identity theft, a law enforcement authority or any other person that the Company has opened a fraudulent account for a person engaged in identity theft

Sample policies and procedures

Detecting and evaluating Red Flags

Policies and procedures for detecting and evaluating Red Flags at the transaction level

Credit applications: All credit applications will be accepted in writing or electronically. Complete or incomplete paper applications should be secured in accordance with the Company's Information Security Program. All credit applications will, at a minimum, contain the following:

- Name
- Date of birth, for an individual
- Address, which shall be:
 - For an individual, a residential or a business street address
 - For an individual who does not have a residential or business street address, an Army Post office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of next of kin or of another contact individual or
 - For a person other than an individual (such as a corporation, partnership or trust), a principal place of business, local office or other physical location
- Identification number, which shall be:
 - For a U.S. person, a taxpayer identification number (such as a Social Security number), including the customer's state of residence at the time of issue or
 - For a non-U.S. person, one or more of the following: a taxpayer identification number (TIN), passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard

Identification verification procedures: The Program Manager will develop a Customer Identification Checklist (attached as Exhibit 2) to be used by Staff responsible for verifying customers' identities each time an Account is opened. The Customer Identification Checklist will be completed with each credit application and maintained with the applicant's credit file. The Program Manager will update such Customer Identification Checklist from time to time as necessary to comply with the terms of this Program.

- **Documentary authentication:** Acceptable documentation for identity verification purposes includes:
 - For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport. Concerns regarding the legitimacy or validity of such identification should be referred to the Program Manager or his or her designee.

Sample policies and procedures

- For business entities (such as a corporation, partnership or trust), documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, partnership agreement or trust instrument. Concerns regarding the legitimacy or validity of such documentation should be referred to the Program Manager or his or her designee.
- **Nondocumentary authentication:** For customers who originate or access Accounts when not physically present in a Company facility, additional steps need to be taken to authenticate their identities:
 - Contact the customer by telephone on at least two occasions prior to opening the Account — once at a home number and once at an office number.
 - Use a third-party identity verification tool to obtain a risk-based score that indicates the likelihood of fraud or identity theft in the transaction.
 - Independently verify the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency. Require the customer to identify:
 - The financial institution holding his or her mortgage, if any, and the total amount of such mortgage
 - The financial institution servicing the customer's current vehicle financing and the remaining balance on the account
 - Issuers of major credit cards most often used by the customer
 - Prior addresses where the customer lived
 - Names of employers
 - Check references with other financial institutions.
 - Obtain a financial statement.
- **Verifying customer-provided information**
 - Validate the customer's SSN using third-party verification tools or other means, such as checking the SSN against the Social Security Administration's Death Master File or validating the first three numbers of the SSN to the state of the customer's residence at the time of issue. If unable to validate the SSN, escalate to the Program Manager or his or her designee for action.
 - If a consumer report is provided with a notice of address discrepancy, ask the customer about the reason for the discrepancy and for additional documentation to verify the address — for example, a utility bill. If unable to validate the address, escalate to the Program Manager or his or her designee for action. In addition, use third-party service providers to determine whether the address provided by the customer is associated with fraud or identity theft. If so, escalate to the Program Manager or his or her designee for action.

Sample policies and procedures

- **Consumer report alert, activity and credit freeze verification**
 - Active duty alerts: If the customer's consumer report contains an active duty alert, attempt to obtain a military ID from the customer as well as orders indicating where he or she is stationed. If the customer is unable to provide either, or the validity of such documents is undeterminable, escalate to the Program Manager or his or her designate for action.
 - Fraud alerts: A customer's consumer report may contain an initial or extended fraud alert. Both instances require additional diligence in the customer identity verification process:
 - An initial fraud alert stays on the consumer report for 90 days and indicates that the customer believes he or she may have been a victim of identity theft. Require additional photo identification and documentation (for example, utility bills, etc.) when verifying the customer's identity. If the consumer report indicates a specific means to be used to identify the customer (e.g., calling the customer at a specific phone number), use that means as well. Document the additional efforts to verify the customer's identity on the Customer Identification Checklist.
 - An extended fraud alert stays on the consumer report for seven years and indicates that the customer has notified the authorities that he or she has been a victim of identity theft. The consumer report will indicate a specific means to be used to identify the customer, and this means must be utilized. Also use the additional verification methods employed in the case of an initial fraud alert. Document the verification on the Customer Identification Checklist.
 - Credit activity: Review all consumer reports carefully for suspicious activity. If any such activity is present, ask the customer about the reasons for such activity. If the customer cannot explain or behaves suspiciously, escalate to the Program Manager or his or her designee for action. Suspicious activity includes:
 - A recent and significant increase in the volume of inquiries
 - An unusual number of recently established credit relationships
 - A material change in the use of credit, especially with respect to recently established credit relationships — for example, significant recent use of existing credit accounts that have otherwise been relatively inactive or only moderately active
 - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor
 - Credit freeze:
 - In the event a consumer report reporting agency indicates that a requested consumer report is subject to a security freeze, advise the customer that he or she will have to provide his or her personal identification number (PIN) to the consumer reporting agency to temporarily thaw the file
 - If the customer does not remember the PIN, direct him or her to the consumer reporting agency for assistance

Sample policies and procedures

- If the customer does not recall his or her PIN and is able to thaw the file after working with the consumer reporting agency, escalate to the Program Manager or his or her designee for action
- Customer/Law Enforcement notices: The Company maintains a file of notices from customers, law enforcement, victims of identity theft and others who have advised of identity theft activity relating to certain names, addresses, phone numbers and SSNs. All Account applications should be checked against such file prior to approval.
- **Existing Accounts:** With respect to the Accounts the Company holds and services, it will take the following actions:
 - In the event of a first payment default, efforts will be made to contact the customer at the addresses and numbers provided to determine the cause for the default. All other Company policies relative to such defaults will be observed. If the customer cannot be contacted and it is believed that a fraud or identity theft has occurred, the Program Manager shall contact law enforcement or take such other action as may be necessary and proper to protect the Company and its customers.
 - In the event of a payment default when there is no history of late or missed payments, efforts will be made to contact the customer at the addresses and numbers provided to determine the cause for the default. All other Company policies relative to such defaults will be observed. If the customer cannot be contacted and it is believed that a fraud or identity theft has occurred, the Program Manager shall contact law enforcement or take such other action as may be necessary and proper to protect the Company and its customers.
 - Upon receipt of a request for a new, additional, or replacement [card or cell phone], or for the addition of authorized users on the Account, the customer should be contacted at the addresses and/or phone numbers on file to verify the request. Such verification should include, as applicable, the use of third-party fraud detection and identity verification tools. In the event the customer identity and new card/cell phone request cannot be verified, escalate to the Program Manager or his or her designee for action.
 - All new Accounts and all existing revolving Account will be monitored for known fraud patterns.

Responding to Red Flags

In general

- Upon detection of a Red Flag, Staff detecting such Red Flag will respond in a manner consistent with the responses detailed in Exhibit 2 or in a manner otherwise consistent with the objectives of this Program.
- In the event there are aggravating circumstances surrounding the detection of a particular Red Flag — for example, the Company has recently experienced a security breach or a theft of customer information — additional diligence should be applied in the customer identification process at the discretion of the Program Manager.

Sample policies and procedures

- In the event any Staff is unable to reconcile a Red Flag with reasonable certainty sufficient to determine the validity of a customer's identity, escalate to the Program Manager or his or her designee for action.
- All Red Flags should be resolved prior to opening or permitting access to an Account. However, Staff may not proceed with a transaction where there is an unresolved Red Flag unless authorized by the Program Manager or his or her designee.

Appropriate responses to Red Flags when opening a covered Account.

Responses to Red Flags detected in the Account opening process typically depend on the facts and circumstances surrounding the Red Flag and require discretion. Typical responses to Red Flags in the Account opening process include:

- Determining that no response is warranted
- Requiring satisfactory explanation from the customer
- Requiring additional identifying documentation from the customer, e.g., additional satisfactory photo identification
- Requiring additional satisfactory identifying information from the customer, e.g., a utility bill showing the customer's name and address or the use of third-party fraud detection and/or identity verification tools
- If the customer's identify can not be authenticated, not opening the Account
- Escalating the Red Flag to the Program Manager for action

Appropriate responses to Red Flags when maintaining a covered Account.

Responses to Red Flags in the Account maintenance process also depend on the facts and circumstances surrounding the Red Flag and require discretion. Typical responses include:

- Determining that no response is warranted
- Contacting the customer to determine the reason(s) for the Red Flag
- For accounts that have phone or Internet access, changing any passwords, security codes or other security devices that permit access to the Account
- Not attempting to collect on an Account that is the result of, or involved in, an identity theft incident and not selling such Account to a debt collector
- Notifying law enforcement

Updating the Program

Review: The Program Manager will review the Program at least once annually and after any significant incidence of identity theft associated with the Company's Accounts.

Sample policies and procedures

Investigation: In the event of a significant incidence of identity theft, the Program Manager will conduct and document an investigation into the facts and circumstances surrounding the incident and recommend changes to the Program.

- The investigation will determine whether:
 - Red Flags already identified in the Program were present in the identity theft incident
 - Current Program procedures for detecting such Red Flags were used in the particular transaction
 - Current Program procedures are sufficient to detect the particular Red Flags
 - Changes to the Program are necessary to identify new Red Flags or detect new or existing Red Flags
 - Additional training for Staff is warranted
- The Program Manager will prepare a report for [The Board of Directors] [The Audit Committee] [Specified individual] as provided in Section III (Program Administration) of this Program after each identity theft incident that was not prevented by the policies and procedures contained in this Program.
- **New methods of identity theft:** As the Program Manager becomes aware of changes in methods of identity theft, he or she will review the Program and recommend any changes that are appropriate.
- **New identity theft detection methods:** As the Program Manager becomes aware of changes in methods to detect and prevent identity theft, he or she will review the Program and recommend any changes that are appropriate. Such methods may include new policies and procedures, as well as implementing risk-based and other technology offerings that are economic and effective.
- **New covered Accounts:** The Program Manager will monitor the financial products and services offered by the Company to determine whether any such products and services are Accounts subject to this Program. Upon determining that a new financial product or service is an Account subject to this Program, the Program Manager will update this Program as appropriate.
- **New and modified business arrangements:** The Program Manager will monitor the business arrangements of the Company, including any mergers, acquisitions, alliances, joint ventures and Service Provider arrangements. The Program Manager will update this Program as appropriate to take into account such changes in the Company's business arrangements.

Sample policies and procedures

Exhibit 1 — Sample

Company Red Flags	Response to Red Flags
Customer receives “low-risk” score from automated customer identification verification tool.	Continue with transaction, provided no other red flags need to be resolved.
Customer receives “medium-risk” score from automated customer identification verification tool.	Proceed to out-of-wallet questions.
Customer receives “high-risk” score from automated customer identification verification tool.	Proceed to out-of-wallet questions and obtain Program Manager approval before originating an account or allowing access to an account.
Customer successfully responds to all out-of-wallet questions.	Continue with transaction, provided no other red flags need to be resolved.
<Additional Red Flags>	
<Additional Red Flags>	
<Additional Red Flags>	
<Additional Red Flags>	

Sample policies and procedures

Exhibit 2— Customer Identification Checklist

Insert institution-specific Customer Identification Checklist

[This page intentionally left blank.]

Conclusion

Conclusion

As of the pre–Nov. 1, 2008, publishing of this paper, the market in general continues to assess the Identity Theft Red Flags and Address Discrepancies Rules under the Fair and Accurate Credit Transactions Act of 2003. On one end of the spectrum are those institutions self-described as fully compliant. At the other end are those institutions becoming aware of the required efforts the guidelines will dictate in their own operations.

Regardless of your institution's position relative to Red Flags readiness, there will be an ongoing need to assess your Identity Theft Prevention Program(s) over time and as dictated by the scope of your activities, products and services provided, and markets served.

Identity fraud, like your prevention programs, will continue to evolve. Via a risk-based approach to fraud detection, prevention and compliance, institutions can incorporate a holistic view of consumer identities and authentication in combination with the nature of the transactions they facilitate. With a varied and predictive set of elements incorporated into a prevention Program comes an inherent ability to more appropriately balance consumer experience, risk mitigation and regulatory compliance.

At their core, the Red Flags guidelines are intended to provide institutions with a more standardized approach to identity theft prevention. As first rounds of examinations occur, and additional best practices surface in the market, institutions should continue to focus on the optimization of their procedures relative to their effectiveness in detecting and preventing fraud while allowing legitimate consumers an unobtrusive means of conducting business.

475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 414 1120
www.experian.com

Hudson Cook, LLP
1020 19th Street, NW
7th Floor
Washington, D.C. 20036



© 2008 Experian Information Solutions, Inc. • All rights reserved

Experian and the marks used herein are service marks or registered trademarks of Experian Information Solutions, Inc.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Experian is a nonexclusive full-service provider licensee of the United States Postal Service®. The following trademarks are owned by the United States Postal Service®: United States Postal Service, USPS, NCOA™. The price for Experian's services is not established, controlled or approved by the United States Postal Service.
USPS Doc # 3.08

10/08 • 2000/1041 • 4827-CS