

Final Rules on Identity Theft Red Flag Alerts and Notices of Address Discrepancies *Will your financial institution be in compliance?*

Beginning November 1, 2008, new rules and guidelines implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) and final rules implementing section 315 of the FACT Act will be mandated for any financial institution and creditor that offers or maintains one or more covered accounts. In addition, any company that pulls credit reports, *i.e.*, auto dealers, security alarm companies and private membership organizations are subject to the same requirements as regulated institutions. Below are questions any organization affected by the new mandate should ask (if you haven't already):

- Do you know which red flags apply to your business?
- Are you adequately protected by your current fraud and compliance solutions?
- Do you have a documented program formalized?
- How can you automate any of these new compliance tasks to minimize additional costs to your bottom line?

What is a Red Flag?

A Red Flag is a pattern, practice or specific activity that indicates the possible risk of identity theft. Indicators of a "possible risk" of identity theft would include precursors to identity theft such as phishing and security breaches involving the theft of personal information which often are a means to acquire the information of another person for use in committing identity theft.

Identifying Relevant Red Flags

Categories of Red Flags – the financial institution or creditor's Program should include relevant Red Flags from the following categories, as appropriate.

- 1) Alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- 2) The presentation of suspicious documents;
- 3) The presentation of suspicious personal identifying information, such as a suspicious address change;
- 4) The unusual use of, or other suspicious activity related to, a covered account; and,
- 5) 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.

Risk Factors - financial institutions or creditors should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

- 1) The types of covered accounts the financial institution or creditor offers or maintains;
- 2) The methods the financial institution or creditor provides to open covered accounts;
- 3) The methods the financial institution or creditor provides to access covered accounts; and,
- 4) The financial institution or creditor's previous experiences with identity theft.

Sources of Red Flags – incorporate relevant Red Flags from sources such as:

- 1) Incidents of identity theft that the financial institution or creditor has experienced;
- 2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and,
- 3) Applicable supervisory guidance.

What is a Covered Account?

Under the final rules, only those financial institutions and creditors that offer or maintain “covered accounts” must develop and implement a written Program. A covered account is (1) an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft. Each financial institution and creditor must periodically determine whether it offers or maintains a “covered account.”

Examples include credit card accounts, mortgage loans, installment credit, margin accounts, cell phone and other utility accounts (extensions of credit), checking and savings accounts. Financial institution risks include financial, operational, compliance, reputation or litigation risks. The regulation covers both existing accounts and those in the process of being opened.

Part of the preliminary and ongoing responsibilities of a financial institution under the regulations will be to, on a risk basis, determine which types of accounts fall into the "other account" group for which there is foreseeable risk of ID theft.

Who is Covered Under the New Guidelines?

The Red Flag regulations and guidelines affect all financial institutions and creditors with covered accounts. "Creditor" includes anyone who arranges for the extension, renewal or continuation of credit (following the definition in the Equal Credit Opportunity Act), which includes automobile dealers, third-party debt collectors and others.

11606 Southfork Ave
Suite 100
Baton Rouge, LA 70816

225.922.4704 [T]
800.568.2027
225.922.4711 [F]
www.noesisdata.com



A financial institution or creditor that uses a service provider to open accounts will need to provide for the detection, prevention or mitigation of identity theft in connection with this activity, even when the service provider has access to the information of a person who is not yet, and may not become, a “customer.”

Who is Protected?

The group of customers whose identity is protected by the regulations and guidelines includes all customers with covered accounts. While the largest group of protected customers is consumers or individuals, the regulations are risk-based, and coverage is extended based on the type of account involved more than on the class of customer.

What should your Program include?

The Program must be designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. In addition, the Program must be tailored to the entity’s size, complexity and nature of its operations. Four basic elements must be included in a financial institution or creditor’s Program. The Program must contain “reasonable policies and procedures” to:

- Identify relevant patterns, practices and specific forms of activity that are “red flags” signaling possible identity theft and incorporate those red flags into the Program.
- Detect Red Flag events that have been included in your Program.
- Respond appropriately to detected Red Flag events to prevent ID theft and mitigate its effects.
- Ensure that the Program is updated periodically to reflect changes in ID theft risks to customers and your institution.

Methods for Administering the Program

One of the steps financial institutions and creditors must take to administer the Program includes oversight. The institution must obtain approval of the initial written Program by the board of directors or an appropriate board committee, ensuring oversight of the development, implementation and administration of the Program, training staff and overseeing service provider arrangements.

11606 Southfork Ave
Suite 100
Baton Rouge, LA 70816

225.922.4704 [T]
800.568.2027
225.922.4711 [F]
www.noesisdata.com

Address Changes (Card Issuers)

The regulations include a requirement that you have policies and procedures to verify address changes for credit card or debit card holders if the address change is followed within 30 days (or a longer period established in your procedures) by a request for an additional card or replacement card for the same account. You can't issue the additional or replacement card until you've checked out the change of address with your cardholder, and provided your cardholder a reasonable means for promptly reporting an incorrect address change.

Your policies and procedures can provide for the verification of all address change requests. If you've already verified such a request before receiving a request for an added or replacement card, you need not verify the address a second time before issuing the card.

What is identifying information?

The FTC defines the term “identifying information” to mean any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

1. Name, social security number, date of birth, office state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
2. Unique biometric data, such as a fingerprint, voice print, retina or iris image or other unique physical representation;
3. Unique electronic identification number, address or routing code; or
4. Telecommunication identifying information or access device.

Don't Delay

With the compliance deadline a short time away, and evidence that examiners have already been asking financial institutions about their Red Flag programs, you should waste no time ramping up your planning for implementation. Be sure your management team and staff understand:

- What industries must comply?
- What are the critical elements of an adequate identity theft prevention program for the scale and scope of your operation?
- Which red flags are relevant for your business?



The next FDIC fraud prevention topic that is currently in the review phase is Accuracy and Integrity of information. Under the FACT Act of 2003, more stringent requirements will be placed on data providers to ensure the accuracy and integrity of information it reports to credit bureaus and to receive and resolve disputes directly. As people find new ways to commit identity theft, more and more will be asked of financial organizations to protect their customers, reputation and bottom line—all with the same few in-house resources. Implementing automated, innovative tools can make the difference between growing a business and defending an examiner's write-up.

There are many customer service tools that can help assess risk, detect fraud, verify identities and assist with consumer disputes. For additional information concerning these solutions and compliance with Red Flag alerts, contact your Noesis Data business consultant at 1-800-568-2027 to learn more.

Layne McDaniel is Chief Executive Officer of Noesis Data, LLC, a company that provides consumer information products and services including credit reports and data products, debt recovery products, fraud detection and prevention, employee background screening, residential tenant screening, check authorization, mortgage reporting, direct marketing, personal solutions and much more. Noesis Data, LLC is an independent sales and marketing representative for the Credit Bureau of Baton Rouge, Inc. and its corporate partners, including Equifax, ChoicePoint, Fidelity National Information Services, AccuData and others. Its relationships with its corporate partners provide clients with the most comprehensive array of consumer information products and services available in the industry (www.noesisdata.com).

11606 Southfork Ave
Suite 100
Baton Rouge, LA 70816

225.922.4704 [T]
800.568.2027
225.922.4711 [F]
www.noesisdata.com