MORRISON | FOERSTER

Legal Updates & News

Legal Updates

Identity Theft Red Flags Rule and Address Discrepancy Rule--Frequently Asked Questions

July 2008
by Andrew M. Smith, Nathan D. Taylor

Related Practices:

- Financial Services Law
- Privacy and Data Security

PDF Version

Identity Theft Red Flags Rule

The federal banking agencies, the National Credit Union Administration (NCUA) and the Federal Trade Commission (FTC) recently have issued a new requirement — called the "Red Flags Rule" — for "creditors" and "financial institutions" to assess whether they offer or maintain "covered accounts," and if they do, to develop and implement an "Identity Theft Prevention Program" (Program) to detect, prevent and mitigate identity theft with respect to those accounts.

When does the Rule take effect?
The Rule took effect on Jan. 1, 2008. Compliance with the Rule, however, is not required until Nov. 1, 2008.

What is a "creditor" under the Rule?
The term "creditor" has the same meaning as under the Equal Credit Opportunity Act (ECOA) and includes a person who regularly participates in credit decisions, including, for example, a mortgage broker, a person who arranges credit or a servicer of loans who participates in "workout" decisions. The term "credit" is defined, as in the ECOA, as the right granted by a creditor to defer payment for goods or services. It is important to note that commercial, as well as consumer, credit accounts may be covered by the Rule. (See "what is a covered account" below.)

What is a "financial institution" under the Rule?
The term "financial institution" is defined as a person that holds a "transaction account" belonging to a consumer. A "transaction account" is an account on which the account holder is permitted to make withdrawals by a negotiable instrument, such as a check. Thus, the term "financial institution" includes a bank, savings association or other depository institution.

We are a "financial institution" for the purposes of the Gramm-Leach-Bliley Act (GLBA). Are we also a "financial institution" under the Red Flags Rule?
Not necessarily. GLBA defines "financial institution" much more broadly than does the Red Flags Rule. Under GLBA, a "financial institution" is "any institution the business of which is engaging in financial activities as described in [the Bank Holding Company Act]," including banks, securities firms, money transmitters and insurers. To be classified as a "financial institution" under the Red Flags Rule, however, you must maintain transaction accounts belonging to consumers.

We are an insurance company that uses credit reports to underwrite insurance. Does the Red Flags Rule apply to us?
The Red Flags Rule should not apply to an insurer when engaged in activities related to insurance underwriting. To the extent that you extend credit, however, you may be covered. For example, you may wish to examine whether you permit consumers to finance their premiums; whether you extend credit to vendors, independent agents or other business partners; or whether you extend credit in

connection with your investment activities, including real-estate investments.

I am an auto dealer. Does the Rule apply to me?
If you extend auto credit to consumers or arrange auto credit for consumers, the Rule may apply.

Does the Rule apply to us even if we do not obtain credit reports?
Yes, if you are a "creditor" or "financial institution," as defined above. The Rule applies to creditors and financial institutions without regard to whether they obtain or use credit reports.

Step 1 — Assessing Whether You Offer Covered Accounts

What is a "covered account"?
A "covered account" is a consumer account offered or maintained by a creditor or financial institution that involves multiple payments or transactions, such as a credit card account, mortgage loan, or checking account. Commercial accounts also can be "covered accounts" where there is a "reasonably foreseeable risk" from identity theft to customers or to safety and soundness.

How do I determine if there is a "reasonably foreseeable risk" from identity theft in a business or commercial account?
Risk is defined to include financial, operational, compliance, reputation or litigation risk. In making your risk determination, you should consider the risk of identity theft presented by the methods that you provide to open business accounts and the methods that you provide to access business accounts, as well as your previous experiences with identity theft, if any, with such business accounts.

Is a commercial real-estate loan a covered account?
Commercial credit accounts can be "covered accounts" if there is a "reasonably foreseeable risk" from identity theft to customers or to safety and soundness.

I service residential mortgage loans. Do I offer or maintain covered accounts?
Residential mortgage loans are covered accounts, and as a servicer you may be considered to be "maintaining" such accounts. Unless, however, you are considered to be a creditor, such as by regularly participating in credit decisions, you are not subject to the Rule. However, you may have contractual duties imposed upon you by the lenders for which you provide services that are related to their Programs.

I am an indirect lender — I do not open accounts directly with a consumer but purchase loans in the secondary market. Am I required to have a Program?
If the loans that you purchase would be considered "covered accounts," you may be required to have a Program. As a secondary market purchaser of loans, however, you may not be considered to "regularly participate" in credit decisions and therefore may not be a "creditor" under the ECOA. In addition, the Rule requires you to address the risks of identity theft in connection with account opening and access. Because you do not originate or "open" accounts but rather purchase them on the secondary market, even if the loans you purchase are "covered" accounts, you should only be required to address the risk of identity theft in connection with account access.

Step 2 — Developing and Implementing a Program

If you are a creditor or a financial institution that offers covered accounts, you must develop a Program to detect possible identity theft in those covered accounts and respond appropriately. The federal banking agencies, the NCUA and the FTC have issued guidelines to help covered entities **identify**, **detect** and **respond** to indicators of possible identity theft, as well as to administer the Program.

Where can I find a copy of the guidelines?

- Federal Reserve Board — 12 C.F.R. pt. 222, App. J
- Federal Deposit Insurance Corporation — 12 C.F.R. pt. 334, App. J
- FTC — 16 C.F.R. pt. 681, App. A
- NCUA — 12 C.F.R. pt. 717, App. J
- Office of the Comptroller of the Currency — 12 C.F.R. pt. 41, App. J
- Office of Thrift Supervision — 12 C.F.R. pt. 571, App. J

Identifying "Red Flags"

What is a "Red Flag"?
A Red Flag is an indicator of the possible existence of identity theft. For example, a Red Flag might be an incorrect or invalid Social Security number (SSN) provided by a consumer applying for a loan. Or, in the case of an existing account, a Red Flag may be an unusual pattern of account usage, such as a credit card being used to purchase an unusually large amount of jewelry, electronics and other easily resold goods.

Does the Rule list the Red Flags?
The Red Flags Rule provides several examples of Red Flags in four separate categories: (1) alerts and notifications received from credit reporting agencies and third-party service providers, (2) the presentation of suspicious documents or suspicious identifying information, (3) unusual or suspicious account usage patterns and (4) notice from a customer, identity theft victim or law enforcement.

How do I know which Red Flags apply to me?
The Red Flags that apply to you depend on a number of factors, including: (1) the types of covered accounts you offer, (2) how those accounts may be opened and accessed and (3) your previous experiences with identity theft. You must consider these factors, as well as various sources and categories of Red Flags identified in the guidelines.

Detecting Red Flags

At which stage of the application process does the Rule apply?
The Rule would apply whenever you detect a Red Flag in connection with an application. This could occur as soon as you receive an application, for example, if the application appears to have been altered or forged or the consumer's identification appears to be forged or is inconsistent with the information on the application.

Is an SSN check a requirement?
No, but an invalid SSN may be a Red Flag — i.e., an indicator of possible identity theft — and obtaining and verifying an SSN may be a reasonable means of addressing this Red Flag when opening an account. You also may be able to utilize your existing procedures under your Customer Identification Program (CIP) under the USA PATRIOT Act.

How are the Red Flags presented on the actual credit report?
The credit reporting agencies will not identify Red Flags as such on a credit report. However, there may be certain information on a credit report that you determine to be an indicator of possible identity theft and you incorporate into your Program, such as a consumer fraud alert or a notice of address discrepancy. In addition, the Guidelines specify that a credit report indicating a pattern of inconsistent or unusual recent activity might be a Red Flag.

We have stopped taking phone applications and are using the out-of-wallet questions for Internet credit applications. Are we going overboard?
The Rule does not preclude phone applications or otherwise limit the manner in which you may accept applications for covered accounts. However, different methods to open covered accounts present different identity theft risks, and you should consider those differing risks in identifying the relevant Red Flags for each type of covered account that you provide.

Responding To Red Flags

What am I supposed to do when I see a Red Flag?
Your Program should include appropriate responses when you detect a Red Flag. You must assess whether the Red Flag evidences a risk of identity theft, and your response must be commensurate with the degree of risk posed. Depending on the level of risk, an appropriate response may include, for example, contacting your applicant or not opening a new account. You also may determine that no response is necessary.

I have detected a Red Flag in connection with a credit application. Am I prohibited from opening the account?
You must assess whether the Red Flag evidences a risk of identity theft, and your response must be commensurate with the degree of risk posed. You are not prohibited from opening the account,

unless the only appropriate response in light of the degree of risk posed by the Red Flag would be not to open the account. In some instances, for example, you may be able to contact the applicant to verify that the application is legitimate.

Would the regulators expect to see a log of detected activity and resulting mitigation?
The Rule does not require you to maintain a log, nor do the Guidelines suggest that a log should be maintained. You are, however, required to prepare regular reports on the effectiveness of your Program, and you also are required to incorporate your own experiences with identity theft when you review and update your Program.

Administering and Updating the Program

A Program must be written, must be approved and implemented by the board of directors, a board committee or senior management, and must include staff training and oversight of service providers. The board of directors or senior management should assign specific responsibility for implementation of the Program, should review reports by staff, and should approve material changes to the Program. Staff should report to the board of directors or senior management at least annually on (1) the effectiveness of the Program's policies, (2) service provider arrangements, (3) significant security incidents and (4) any recommendations for material changes.

Does the Program have to be approved by the board annually?
No, but the board (or a committee of the board) or senior management must annually review reports prepared by staff regarding your Program and must approve any material changes to that Program.

Can I tie this in with the bank's Customer Identification Program (CIP) so as not to overburden our staff with more rules to follow?
You may incorporate your CIP procedures into your Program to the extent that it is appropriate. For example, your CIP procedures likely would assist you in detecting relevant Red Flags in connection with new covered accounts but not with respect to existing accounts.

Address Discrepancy Rule
The nationwide credit reporting agencies — Experian, TransUnion and Equifax — are required to notify you when an address in their credit file for a consumer "substantially differs" from the address that you provide for the consumer when you request the credit report. New rules from the federal bank agencies and the FTC require you to confirm the identity of the consumer when you receive an address discrepancy notice from a credit reporting agency. These rules also may require you to reconcile the address provided by the consumer with the address in the credit reporting agency's file, but only if you regularly furnish information to that credit reporting agency. Fair Credit Reporting Act § 605(h) — 15 U.S.C. § 1681c(h); Federal Reserve Board — 12 C.F.R. § 222.82; Federal Deposit Insurance Corporation — 12 C.F.R. § 334.82; FTC — 16 C.F.R. § 681.1; NCUA — 12 C.F.R. § 717.82; Office of the Comptroller of the Currency — 12 C.F.R. § 41.82; Office of Thrift Supervision — 12 C.F.R. § 571.82.

How do the credit reporting agencies display an address discrepancy?
Each credit reporting agency displays an "address discrepancy indicator," which typically is simply a code in a specified field. Each credit reporting agency uses a different indicator.

How do we "form a reasonable belief" that a credit report relates to the consumer for whom it was requested?
Following procedures that you have implemented as a part of your Customer Identification Program under the USA PATRIOT Act would satisfy this requirement. You also can compare the credit report with information in your own records or information from a third-party source, or you may verify information in the credit report with the consumer directly.

If a credit report is pulled on a loan applicant who is not our customer, and there is an address discrepancy on the credit report, are we obligated to resolve the discrepancy if the loan is denied?
You are only required to reconcile the address with the credit reporting agency if you "establish a continuing relationship with" the consumer.

We do not regularly furnish data to any credit reporting agency. Are we required to furnish the consumer's correct address?
If you do not regularly furnish data to a credit reporting agency in the ordinary course of your

business, there is no obligation to report correct addresses.

When do we communicate the corrected address to the credit reporting agency?
You must furnish the verified address to the credit reporting agency with the other account data that you furnish to that credit reporting agency for the reporting period in which you establish the relationship with the consumer.