



July 27, 2006

FACT Act Guidelines and Rules on Identity Theft “Red Flags” and Change of Address Discrepancies

EXECUTIVE SUMMARY

- The National Credit Union Administration (NCUA) and the other financial institution regulators, as well as the Federal Trade Commission (collectively the “Agencies”), have issued proposed guidelines that identify “red flags,” which are patterns, practices, or activities that indicate the possible risk of identity theft, along with proposed rules requiring financial institutions and other creditors to implement the guidelines. The guidance and rules are required under the Fair and Accurate Credit Transactions Act, which was enacted in 2003.
- The guidelines and rules issued by NCUA will apply to federally-chartered credit unions, and the guidelines and rules issued by the Federal Trade Commission will apply to state-chartered credit unions, although these rules are essentially the same.
- The proposed guidelines list a number of “red flags” that may indicate identity theft. This includes the existence of fraud alerts, altered and inconsistent information, account use that fits a pattern of fraud, notifications of unauthorized charges or fraudulent account charges, returned mail or e-mails, attempts to access accounts by unauthorized users, as well as a number of other indicators.
- The proposed rules adopt a risk-based, flexible approach that will require creditors to have a written identity theft prevention program that is appropriate to the size and complexity of the institution, as well as the nature and scope of its activities. This program will require a number of components, such as reasonable policies and procedures, staff training, oversight of service providers, and oversight by the board of directors.

- The proposed rules will also require credit and debit card issuers to establish reasonable policies and procedures to assess the validity of a change of address when there is also a request for an additional or replacement card within a short period of time, which is often an indication of identity theft. In this situation, the card issuer may not issue another card without notifying the cardholder at the former address or using some other means to verify the change. Also, users of consumer reports who receive a notice of an address discrepancy from a credit bureau must have procedures in order to form a reasonable belief of the consumer's identity. The user must also have policies and procedures in place when furnishing an address to the credit bureau that the user believes is accurate.
- Comments in response to the proposal are due by September 18, 2006.
Please submit your comments to CUNA by September 7, 2006.

Please feel free to fax your responses to CUNA at 202-638-7052; e-mail them to Senior Vice President and Deputy General Counsel Mary Dunn at mdunn@cuna.coop and to Senior Assistant General Counsel Jeff Bloch at jbloch@cuna.coop; or mail them to Mary and Jeff in c/o CUNA's Regulatory Advocacy Department, 601 Pennsylvania Avenue, NW, South Building, Suite 600, Washington, DC 20004-2601. You may also contact us at 800-356-9655, ext. 6732, if you have questions or would like a copy of the proposal. You may also access a copy of the proposal at the following address:

http://www.ncua.gov/RegulationsOpinionsLaws/proposed_regs/P-J-717.pdf

BACKGROUND

The FACT Act was enacted in December 2003 and includes a number of provisions that address the detection and prevention of identity theft. These include a requirement that the Agencies jointly issue guidelines for financial institutions and other creditors with regard to identity theft. These guidelines must identify patterns, practices, and specific activities that indicate the possible existence of identity theft.

The FACT Act also requires the Agencies to issue rules requiring financial institutions and other creditors to establish policies and procedures for implementing the guidelines that identify possible risks to consumers or risks to the safety and soundness of the institution. The rules must also require credit and debit card issuers to assess the validity of change of address requests when there is also a request for an additional or replacement card, which is often an indication of identity theft. Specifically, the card issuer must follow reasonable policies and procedures to determine the validity of a change of address request if it receives the request for an existing account and within a short period of time (at least 30 days) receives a request for an additional or replacement card for that account.

Under these circumstances, the card issuer must not issue a card unless it:

- notifies the cardholder of the request at the cardholder's former address and provides the cardholder with a means to promptly report an incorrect address;
- notifies the cardholder of the address change request by another means of communication previously agreed to by the issuer and cardholder; or
- uses other means of evaluating the validity of the address change, in accordance with the issuer's reasonable policies and procedures.

The FACT Act also requires the nationwide credit bureaus to provide a notice of address discrepancy if the address provided by the user in its request for credit information differs substantially from the address that the credit bureau has in its files.

As required under the FACT Act, the Agencies have proposed guidelines that identify patterns, practices, and specific forms of activity that indicate a possible risk of identity theft (referred to as "Red Flag Guidelines"). The Agencies have also proposed rules requiring each financial institution to implement a written Identity Theft Prevention Program (Program), which must contain reasonable policies and procedures that address the risk of identity theft. These rules also require financial institutions to incorporate relevant indicators of identity theft into their programs from among those outlined in the Red Flag Guidelines.

The Agencies have also proposed rules to require credit card issuers to implement the reasonable policies and procedures to address the validity of a change of address, as required under the FACT Act, as well as rules that provide guidance on policies and procedures that a user of credit reports should use if it receives a notice of address discrepancy from one of the nationwide credit bureaus.

BRIEF DESCRIPTION OF THE PROPOSED RULES AND GUIDELINES

Proposed Red Flag Rules

The Red Flag rules require each financial institution or creditor to implement a written Program that outlines reasonable policies and procedures to address the risk of identity theft to consumers and to the safety and soundness of the financial institution or creditor. This includes addressing the financial, operational, compliance, reputation, and litigation risks.

The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. It is, therefore, designed to be flexible and to take into account the operations of smaller institutions. The Program may also be combined with the institution's existing information security program.

The Program must also address changing identity theft risks as they arise, based on the experience of the institution with identity theft, as well as address the changes in the methods of identity theft, the methods to detect and mitigate identity theft, the changes in the types of accounts offered, and changes in its business arrangements. This will require each institution to monitor, evaluate, and adjust its Program and types of accounts offered, as appropriate.

The Program must include policies and procedures to identify which “red flags,” either alone or in combination with other “red flags,” are relevant in detecting the possible risk of identity theft to consumers or to the safety and soundness of the institution. “Red flags” are patterns, practices, or activities that indicate the possible risk of identity theft. In identifying the relevant “red flags,” the institution must consider the following factors, which are very similar to those that need to be considered when verifying the identity of consumers opening new accounts under the Customer Identification Program (CIP), as required under the Patriot Act:

- Which of its accounts are subject to the risk of identity theft.
- The methods it provides to open these accounts.
- The methods it provides to access these accounts.
- The institution’s size, location, and customer/member base.

The “red flags” identified must reflect changing identity theft risks to consumers and to the institution as they arise. The Program must incorporate relevant “red flags” from the following sources:

- The *Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation* that is incorporated as an appendix to these proposed rules.
- Any applicable supervisory guidance, either now or in the future.
- Incidents of identity theft that the creditor has experienced.
- Methods of identity theft that the creditor has identified that reflect changes in identity theft risks.

The Program must include policies and procedures designed to prevent and mitigate identity theft in connection with the opening of an account or an existing account. This includes policies and procedures to:

- Obtain verifying information about, and verify the identity of, a person opening an account. Using the policies and procedures for identification and verification that are required under the CIP rules will satisfy this requirement.
- Detect the “red flags” that have been identified in the Program and determine whether they indicate a risk of identity theft. The institution must have a reasonable basis for concluding that a “red flag” does not evidence such a risk.
- Address the possible presence of identity theft, commensurate with the degree of risk posed, which may include:
 - Monitoring an account for evidence of identity theft.
 - Contacting the consumer.

- Changing passwords, security codes, or other devices that permit access to an account.
- Reopening an account with a new account number.
- Not opening a new account.
- Closing an existing account.
- Notify law enforcement and possibly filing a Suspicious Activity Report.
- Implementing requirements for limiting credit extensions, such as declining to issue an additional card if there is a fraud or active duty alert on the credit report.
- Implementing requirements that a furnisher of credit information to a credit bureau has for correcting or updating inaccurate information.

Each creditor must train staff to implement the Program. Also, whenever an institution engages a service provider to perform an activity covered under the Program, such as opening an account, the institution must ensure that the activity is in compliance with a Program that meets the requirements of these “red flag” rules.

The board of directors, or an appropriate committee of the board, must approve the written Program. The board, the appropriate committee, or senior management must oversee the development, implementation, and maintenance of the Program.

The staff responsible for implementing the Program must deliver an annual report to the board, the appropriate committee, or senior management regarding compliance by the institution with the “red flag” rules. The report must evaluate issues such as the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening an account or an existing account, service provider arrangements, significant incidents involving identity theft and management’s response, and recommendations for changes to the Program.

Proposed Red Flag Guidelines

The Agencies have included “red flag” guidelines as an appendix to these rules, titled *“Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation.”* These guidelines include a list of “red flags” in connection with an account opening or an existing account. As mentioned above, the Program adopted by the institution must include policies and procedures to identify “red flags” relevant to detecting a possible risk of identity theft from among those listed in this appendix. Some of the “red flags” may, by themselves, be reliable indicators of identity theft, while others may be more reliable when detected in combination with other “red flags.”

Here is the list of “red flags” that are outlined in the appendix, which is not intended to be an exhaustive list of all possible “red flags”:

- A fraud or active duty alert on the credit report.

- A notice of address discrepancy provided by a credit bureau.
- The credit report or a use of an account that indicates a pattern of activity inconsistent with the history or pattern of activity usually associated with the consumer.
- Documents provided for identification that appear to be altered.
- The photograph, description of the consumer, or other information on the identification is inconsistent with the appearance of the consumer who is presenting the identification.
- The information on the identification or other personal information is not consistent with information that is on file.
- Personal information provided is inconsistent when compared to external information sources.
- Personal information is internally inconsistent, such as a Social Security number that is inconsistent with a consumer's date of birth.
- Personal information that has also been provided on a fraudulent application.
- Personal information associated with fraudulent activity, such as an invalid address and phone number.
- Address, Social Security number, and phone numbers that have been submitted by other consumers.
- The consumer failing to provide all required information on an application.
- The consumer cannot provide authenticating information, other than what would be available from a wallet or credit report.
- There is a request for additional authorized users for an account or a request for new, additional, or replacement cards and checks shortly after a request for a change of address.
- Mail is returned undeliverable even though transactions on the account continue to be conducted.
- A new, revolving credit account is used in a manner associated with fraud, such as credit used for cash advances or for merchandise that is easily converted to cash, or the consumer fails to make payments.
- When an account is being used after being inactive for a long time.
- The institution is notified of unauthorized charges, that it has opened a fraudulent account, that the consumer is not receiving account statements, or that the consumer has provided information to a fraudulent website or to someone fraudulently claiming to represent the creditor.
- E-mails not sent by the institution are returned to the e-mail server of the creditor.
- An employee of the institution is added as an authorized user of an account.
- An employee has accessed an unusually large number of consumer accounts.
- The institution detects attempts by an unauthorized person to access the consumer's account.
- The institution detects or receives information of unauthorized access to the consumer's personal information.

- There are unusually frequent and large check orders in connection with a consumer's account.
- A person opening an account is unable to lift a credit freeze placed on his or her credit report.

Proposed Rules Regarding Change of Address Discrepancies

These proposed rules, which apply to credit and debit card issuers, state that a card issuer may not issue an additional or replacement card if such a request is received within a short time period (which must be at least 30 days) after receiving notification of a change of address for that account, unless the issuer assesses the validity of the change of address request. Under these circumstances, in accordance with its policies and procedures for determining the validity of the request, the card issuer must:

- notify the cardholder of the request at the cardholder's former address and provide the cardholder with a means to promptly report an incorrect address;
- notify the cardholder of the address change request by another means of communication previously agreed to by the issuer and the cardholder; or
- use other means of evaluating the validity of the address change, in accordance with the issuer's policies and procedures that are outlined in its Program, as described in the proposed "red flag" rules described above.

Any written or electronic notice that is provided under these rules must be "clear and conspicuous" and provided separately from the regular correspondence that is sent to the consumer. The definition of "clear and conspicuous" is the same as used in the Agencies privacy rules, which is "reasonably understandable and designed to call attention to the nature and significance of the information." Oral notices may also be provided, if outlined in the policies and procedures that the issuer has established pursuant to the "red flag" rules.

Proposed Rules on Duties of Users of Credit Reports Regarding Address Discrepancies

The user of credit report information must use reasonable policies and procedures for verifying the identity of the consumer for whom it has obtained a credit report whenever the user receives a notice of an address discrepancy from a credit bureau. The policies and procedures must enable the user to form a reasonable belief that it knows the identity of the consumer or determine that it cannot form such a belief. Using the policies and procedures regarding identification and verification that are outlined in the CIP rules will satisfy this requirement. Such a notice is also a "red flag" and, therefore, the users Program that is developed under the "red flag" rules may apply here.

When the following conditions are satisfied, a user must also use reasonable policies and procedures for furnishing to the credit bureau, from whom it received

a notice of address discrepancy, the address for the consumer that the user has reasonably confirmed is accurate:

- The user can form a reasonable belief that it knows the identity of the consumer for whom the credit report was obtained.
- The user establishes or maintains a continuing relationship with the consumer.
- The user regularly and in the ordinary course of business furnishes information to the credit bureau from which the notice of address discrepancy was obtained.

The user may reasonably confirm that an address is accurate by any of the following:

- Verifying the address directly with the consumer.
- Reviewing its own records of the address that was provided in requesting the credit report.
- Verifying the address through third party sources.
- Using other reasonable means.

For new relationships, the user's policies and procedures must require that the user will furnish the address that it confirms as accurate to the credit bureau for the reporting period in which it establishes the relationship with the consumer. For other circumstances, such as when there is already an existing relationship with the consumer, the user should furnish the information for the reporting period in which the user confirms the accuracy of the address.

**QUESTIONS TO CONSIDER REGARDING THE GUIDELINES AND RULES
ON "RED FLAGS" AND CHANGE OF ADDRESS DISCREPANCIES
(The Agencies have specifically requested comment on the
issues raised in these questions.)**

- "Red flags" are generally defined as patterns, practices, or activities that indicate the possible risk of identity theft. This would include situations in which there is a "possible" risk of identity theft, even though the existence of identity theft is not necessarily indicated, such as the receipt of a "phishing" e-mail or a security breach. Should the definition of "red flags" include these possible risks of identity theft?

- The financial institution’s Program must incorporate relevant “red flags” from: 1) the *Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation* that is incorporated as an appendix to the proposed rules; 2) any applicable supervisory guidance, either now or in the future; 3) incidents of identity theft that the institution has experienced; and 4) methods of identity theft that the institution has identified that reflect changes in identity theft risks. Are these appropriate sources?

- A financial institution using a third party’s computer-based programs to detect identity theft must independently assess whether the programs meet the requirements of these rules and should not rely on the representations of the third party. What impact will this have on the policies and procedures that you currently have to detect and mitigate identity theft, including on third party computer-based products that you currently use?

- In identifying the relevant “red flags” for its program, the institution must consider which of its accounts are subject to the risk of identity theft; the methods it provides to open these accounts; the methods it provides to access these accounts; and its size, location, and customer/member base. Are these factors appropriate and should any others be considered?

- The proposed rules include a number of actions that a financial institution may take to address the risk of identity theft, such as monitoring an account for evidence of identity theft; contacting the consumer; changing passwords, security codes, or other devices that permit access to an account; reopening an account with a new account number; not opening a new account; closing an existing account, notifying law enforcement, and possibly filing a Suspicious Activity Report; implementing any requirement for limiting credit extensions, such as declining to issue an additional card if there is a fraud or active duty alert on the credit report; and implementing any requirement that a furnisher of credit information to a credit bureau has for correcting or updating inaccurate information. Should these all be included as examples and are there any other appropriate examples?

- Would it be appropriate to allow a service provider to implement a Program that may be different from the one developed by the financial institution? Is it necessary to address service provider arrangements in these rules or would it be self-evident that the institution would be responsible for complying with these rules, even if they contract with a service provider to perform these activities?

- Will annual reports to the board, a board committee, or senior management regarding compliance with these rules be sufficient? Are the responsibilities allocated between the board and senior management regarding the required oversight and reporting of the Program sufficient?

- Are the “red flags” listed in the proposed guidelines, which will be outlined in the appendix to these rules, too specific or not specific enough? Should additional or different ones be included?

- One of the “red-flags” listed is when an account is being used after being inactive for a long time. The FACT Act indicates that the account should be inactive for two years before it should be considered a concern. Should the rules include the two-year time period or should a time period not be listed to take into consideration the different types and usage of various accounts?

- When required to determine the validity of a request for an additional or replacement credit or debit card shortly after receiving a change of address request, the card issuer must either: 1) notify the cardholder of the request at the cardholder’s former address and provide the cardholder with a means to promptly report an incorrect address; 2) notify the cardholder of the address change request by another means of communication previously agreed to by the issuer and cardholder; or 3) use other means of evaluating the validity of the address change. Is further elaboration needed regarding these means of verifying a change of address request?

- Any written notice to consumers regarding change of address discrepancies must be clear and conspicuous and separate from the regular correspondence to the cardholder. Should there be further elaboration regarding these notices?

- The user of credit report information must use reasonable policies and procedures for verifying the identity of the consumer for whom it has obtained a credit report whenever the user receives a notice of address discrepancy from a credit bureau. Using the policies and procedures regarding identification and verification that are outlined in the CIP rules will satisfy this requirement. Are these CIP procedures sufficient?

- When certain conditions are satisfied, a user of credit information must use reasonable policies and procedures for furnishing to the credit bureau, from whom it received a notice of an address discrepancy, the address for the consumer that the user has reasonably confirmed is accurate. Methods to do so include verifying the address directly with the consumer, reviewing its own records of the address that was provided in requesting the credit report, verifying the address through third party sources, or using other reasonable means. Should these methods be included and are there other methods that should be included?

- For new relationships, the user of the credit information will furnish the address that it confirms as accurate to the credit bureau for the reporting period in which it establishes the relationship with the consumer. For other circumstances, such as when there is already an existing relationship with the consumer, the user should furnish the information for the reporting period in which the user confirms the accuracy of the address. Are these time periods appropriate?

- Other comments?
