CUNA
Credit Union National Association
601 Pennsylvania Ave., NW | South Building, Suite 600 | Washington, DC 20004-2601 | PHONE: 202-638-5777 | FAX: 202-638-7734
cuna.org

September 18, 2006

Federal Trade Commission
Office of the Secretary
Room 159-H (Annex C)
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: The Red Flags Rule – Project No. R611019

Dear Sir or Madam:

The Credit Union National Association (CUNA) appreciates the opportunity to comment on the 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 (FACT) Act, with the Federal Trade Commission (FTC) being responsible for issuing rules for state-chartered credit unions and the National Credit Union Administration (NCUA) responsible for rules that will apply to federally-chartered credit unions. We are filing a virtually identical letter with the FTC. CUNA represents approximately 90 percent of our nation's 8,800 federal and state-chartered credit unions, which serve nearly 87 million members.

Summary of CUNA's Comments

- These rules do not address the significant problem with regard to identity theft, which is data security vulnerabilities, as evidenced by the larger number of security breaches that have occurred in recent years. We urge the FTC and the other agencies to increase their focus on this issue as a means to address the security breach problem. One means to address this issue would be a "summit" hosted by the regulators for the various stakeholders to express concerns and offer recommendations.
- These regulatory requirements are in many ways duplicative of the requirements in the Customer Identification Program (CIP), as required under the USA PATRIOT Act. Although the FTC and the other agencies have indicated that compliance with the CIP will be sufficient for purposes of complying with certain requirements in this

proposal, we believe the preferable approach would be to eliminate the redundancies between these rules and the CIP rules.

- CUNA is concerned about the cumulative regulatory burden associated with the rules that have been enacted under the FACT Act. In that connection, it is important that the FTC and the other regulators agree to review the rule's impact and the cumulative FACT Act compliance burden one year after compliance is required with this rule and periodically thereafter as a means to address unnecessary burdens.
- CUNA is also concerned that there will be an expectation that all of the identity theft "red-flags" either be incorporated into the identity theft program, which credit unions and others will be required to develop under these rules, or these institutions will have to provide justification for not incorporating those red-flags that are not included in the program. The rules and guidelines should state clearly that there will be no expectation from regulators that all of the red-flags must be included in an institution's identity theft program. Further, there should be guidance provided from the regulators on what specific issues examiners will be focusing on when they assess compliance with these rules.
- The FTC and the other agencies issuing the rules and guidelines have defined "red-flags" to include precursors to identity theft that indicate a "possible" risk. Although we do not disagree with this definition, we are concerned as to how this could apply in certain situations. An example would be that the receipt of a "phishing" email should not necessarily be a red-flag without some other indicator, such as the consumer responding to the email and providing sensitive information.
- Although financial institutions should be responsible for compliance with the rules, even if they use service providers, it is not necessary to specify in the rules the methods through which institutions would ensure compliance by these service providers.
- Although we do not necessarily object to the requirement that annual reports be provided to the board of directors, a board committee, or senior management regarding compliance with these rules, we question the need for board approval, and believe no other affirmative duties should be placed on the board with regard to these rules.
- The proposed rules will also require that a written notice to consumers regarding change of address discrepancies must be "clear and conspicuous" and separate from the regular correspondence to the cardholder. We do not believe it is necessary to include a "clear and conspicuous" requirement as these notices will be sent separately from regular correspondence and should be rather brief.
- We offer numerous, specific suggestions with regard to many of the red-flags that are listed in the guidelines.

- Compliance should not be required until at least eighteen months after the final rules are issued to ensure that credit unions have sufficient time to review and analyze their existing operations and to make the necessary changes.
- The agencies estimate it will take financial institutions 25 hours to create an identity theft program, four hours to prepare an annual report, and two hours to train staff. We question the estimate as detailed analysis has not been provided in this proposal to substantiate them. We are concerned that they do not reflect the scope of the burden on institutions, particularly smaller ones that will be required to comply with these rules.

Discussion of CUNA's Comments

We support the efforts of the FTC and the other financial institution regulators to develop rules that address the growing problem of identity theft. In general, CUNA recognizes that the proposal has been designed to afford credit unions and others with significant flexibility in developing their required identity theft programs, based on their size and complexity of their operations. Many credit unions have already been subject to fraud and identity theft problems and currently have procedures in place that meet a number of the requirements outlined in the rules, which are intended to protect against such fraud, as well as to comply with current anti-money laundering rules.

Many of the red-flags listed in the guidelines are fairly common and widely recognized by credit unions and others as indicia of identity theft, with common examples being documents that appear to be altered and situations in which the appearance of the person providing the identification documentation is different from the picture that appears on the documentation. However, although we generally support the agencies' efforts, we do have some concerns and offer suggestions for your consideration.

One of CUNA's significant concerns is that these rules do not address the underlying problem of data security vulnerabilities, which can result in identity theft, as evidenced by the larger number of security breaches that have occurred in recent years. We urge the FTC and the other agencies to work more closely with Congress, card issuers, financial institutions and consumers to focus on the security breach problem. One way to accomplish this goal of bringing the principal stakeholders together would be for the agencies to hold a "summit" and invite stakeholders to address concerns and offer recommendations to help safeguard financial data.

Another concern is that these regulatory requirements are in many ways duplicative of the CIP requirements, as required under the USA PATRIOT Act. Although the FTC and the agencies have indicated that compliance with the CIP will be sufficient for purposes of complying with certain requirements in this proposal, we believe the preferable approach would be to eliminate the redundancies between these rules and the CIP

rules. Otherwise, credit unions will be concerned that examiners will require them to comply separately with the CIP rules and the red-flag rules, even though the proposal will allow CIP compliance to substitute for certain of the requirements under these rules.

The need to avoid duplication is also necessary because of the cumulative regulatory burden associated with the rules that have been enacted under the FACT Act. Because of this burden, it is important that redundancies be limited, and it also important that the FTC and the other regulators periodically review these rules as a means to reduce unnecessary burdens. Although the agencies conduct periodic regulatory reviews, we believe special emphasis should be placed on reducing the cumulative burdens associated with the FACT Act rules. The first such review should take place one after compliance with this rule is required, and periodically thereafter.

CUNA's general concern with the rules and guidelines is that there will be an expectation that all of the "red-flags" either be incorporated into the identity theft program, which credit unions and others will be required to develop, or these institutions will have to provide justification for not incorporating those red-flags that are not included in the program. The rules clearly indicate that the identity theft 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.

To expect a financial institution to develop and provide information to justify not using any particular red-flag would impose significant burdens on the institution. The result may be that an institution may include all or most of the red-flags that are listed in the guidelines as means to avoid this burden. This would clearly contravene the goal that these identity theft programs be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. This would also contravene the requirement in the rules that the program take into account the changing identity risks as they arise, since an institution may not make these changes if it would be required to justify the deletion of a red-flag.

To avoid this result, we urge the FTC and the other agencies to clearly state there is no expectation that a financial institution would include a red-flag listed in its identity theft program that it believes would not be necessary. The agencies should also indicate that they expect the red-flags to change over time, resulting in the deletion of red-flags that may become outdated in the future. There should also be guidance provided from the regulators on what specific issues examiners will be focusing on when they assess compliance with these rules.

The FTC and the other agencies have defined "red-flags" to include precursors to identity theft that indicate a "possible" risk. Although we do not disagree with this definition, we are concerned as to how this could apply in certain situations. For example, "phishing" can clearly lead to identity theft problems, since this is an attempt in which a fraudster sends a spam email directing consumers to a bogus

website in an attempt to trick them into providing sensitive information. However, while fraudsters use phishing to lure unsuspecting consumers, a phishing attempt by itself would not necessarily be a precursor to identity theft. We believe it would not be a precursor unless and until the consumer responds to the phishing attempt and provides sensitive information. At that time, we would agree this would be a precursor to identity theft, even if the fraudster does not or is unable to use that information at a later time to commit identity theft.

However, there would have to be a distinction between consumers who notify the institution that they have responded to a phishing attempt and consumers who notify the institution of other circumstances in which they believe presents an identity theft problem. For example, a consumer may notify the institution that they have lost a check or a credit card. We do not believe this should be considered a red-flag, since in most situations these examples would not result in an identity theft problem. Financial institutions should continue to provide the protections they currently offer in these situations, but these examples should not be included as a red-flag under these rules. The distinction between these examples and phishing would be that a phishing attempt is clearly an action by a fraudster, which is not apparent in these other examples.

Under the proposed rules, a financial institution using a third party's computer-based programs to detect identity theft must independently assess whether the program meets the requirements of these rules and should not rely on the representations of the third party. This could have an adverse affect for many credit unions, especially smaller credit unions that simply do not have the means to assess on their own whether these third-party programs are in compliance with these rules. These credit unions would, therefore, be at a significant disadvantage, as compared to larger financial institutions that either have their own programs or the means to independently assess a third-party's program.

To alleviate this possible adverse affect, the FTC and the other regulators should clarify that financial institutions can comply with this requirement of independently assessing third-party programs through a variety of means. One would be to allow groups of credit unions that use a specific provider to obtain and rely on the opinion of an outside firm that would be responsible for assessing the third-party's program. In a similar situation, credit unions were permitted to enter these arrangements in order to test systems for Year 2000 compliance.

The other alternative would simply be to delete this type of requirement in the rule, with the understanding that the institution would be responsible for compliance, and permit the institutions to mitigate the damages and penalties for noncompliance by way of warranties that would be included in the contract with the service provider or through other means. This approach of not specifically mentioning the obligations with regard to service providers could apply to all aspects of the rules and guidelines.

The FTC and the other agencies have also requested comment as to whether annual reports to the board of directors, a board committee, or senior management regarding compliance with these rules are sufficient. Although we do not necessarily object to these reports, we question the need for board approval, and believe no other affirmative duties should be placed on the board with regard to these rules. This not only creates additional burden on the board, but may also inhibit changes to the program that address new risks if there is a requirement that these changes also have to be approved.

As for the requirement 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 proposed rules will require the card issuer to: 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. Although not currently used on widespread basis, we believe electronic communications may become a very useful means for evaluating the validity of an address change. Specifically, an email sent by the consumer to the institution, along with a valid electronic signature, should be sufficient to indicate that the address change request is legitimate, without the need for an additional notification requirement.

The proposed rules will also require that any written notice to consumers regarding change of address discrepancies must be "clear and conspicuous" and separate from the regular correspondence to the cardholder. We do not believe it is necessary to include a "clear and conspicuous" requirement. This notice will be sent separately from regular correspondence and should be rather brief, as it is only intended to communicate the request for a change of address. Such a separate, brief notice should in and of itself be considered "clear and conspicuous."

To add a specific "clear and conspicuous" requirement will also raise concerns as to how this will be interpreted and whether it will be interpreted consistently among the FTC and the other agencies. This additional requirement may also imply specific font, type size, spacing, and content requirements, which again should be unnecessary for what should be a relatively short notice.

Here are our comments in response to a number of the specific red-flags that are listed in the guidelines:

- A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity, such as an account closed or identified for abuse of account privileges – This would not necessarily be an indication of identity theft. This specific situation should be removed or the FTC and the other agencies should provide more information as to the context of how this would be a red-flag.

- Personal information provided is inconsistent with external information sources – The FTC and the other agencies should clarify that this refers to inconsistencies due to fraud, as opposed to inconsistencies as a result of typographical errors or other "innocent" mistakes.
- Personal information provided that is internally consistent, such as a lack of correlation between the social security number (SSN) range and the date of birth – The term "internally inconsistent" should be defined. Also, it would be very burdensome for credit unions to be responsible for validating the accuracy of a SSN for purposes of being able to correlate the information to the birth date.
- The address, SSN, or home or cell phone number provided is the same as that submitted by others – Address and phone numbers change frequently and, therefore, it may not necessarily be an indicator of identity theft if this information was the same as those submitted by others. This should not be considered a red-flag.
- Consumer fails to provide all required information on an application – There are a number of reasonable explanations in which a consumer may not be able to provide this type of information. These include when the consumer recently has moved and may not remember the address, the consumer is preoccupied with personal and family emergencies that may cause lapses of memory, as well as the reality that many people often do not remember certain information, such as SSNs and phone numbers. For these reasons, we believe this should not be included as a red-flag.
- Consumer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report – We believe this red-flag should specifically indicate that the authenticating information would include any prearranged verification methods that have been agreed to by the consumer and the financial institution. Common methods include providing a password or mother's maiden name, although neither these nor other specific examples should be included as these methods vary among institutions and may change over time.
- Mail sent to the consumer is returned as undeliverable, even though transactions continue to be conducted with the consumer's account – Many consumers often forget to submit a change of address to the post office when they move. This is a very common occurrence and, therefore, this red-flag should indicate that there needs to be some other indicia of possible identity theft in order for this to be of concern.
- An account is used in a manner commonly associated with fraud, such as the consumer failing to make the first payment or makes an initial payment but no subsequent payments – Failing to make payments is not necessarily an indication of identity theft and, therefore, this should be removed as a red-flag.
- Inactive accounts - one of the "red-flags" listed is when an account is being used after being inactive for a long time. We believe the term "inactive" is too vague. For example, this may mean a time period in which there are no purchases, advances, balance transfers, and other activities, even if the consumer is making payments on previously incurred debt, or this may mean a time period in which there is no activity at all. We believe "inactive" should mean no activity whatsoever

and would include an account as active even if the only activity was the consumer downloading an account statement through a home banking system. Also, the Fair and Accurate Credit Transactions Act indicates that an account should be inactive for two years before it should be of concern. We believe this two-year period should be included within this red-flag. Otherwise, different regulators and examiners may impose different time periods, leading to inconsistencies among financial institutions.

- The financial institution or creditor is notified that the consumer is not receiving account statements – This red-flag needs to be clarified. Again, many consumers neglect to submit a change of address form with the post office when they move, which may cause them to not receive these statements. Also, many consumers are now opting to receive statements electronically and, therefore, this red-flag should clarify that not receiving account statements by postal mail does not necessarily indicate identity theft.

In order to allow credit unions sufficient time to comply with these new rules and guidelines, we request that the FTC and the other agencies provide a required compliance date that is no less than eighteen months after the final rules are issued. This will be necessary to ensure that credit unions have sufficient time to review and analyze their existing operations and to make the necessary changes.

The agencies estimate it will take financial institutions 25 hours to create an identity theft problem, four hours to prepare an annual report, and two hours to train staff. We question the estimate as detailed analysis has not been provided in this proposal to substantiate them. We are concerned that they do not reflect the scope of the burden on institutions, particularly smaller ones that will be required to comply with these rules.

Thank you for the opportunity to comment on these proposed rules and guidelines. If Board members or agency staff have questions about our comments, please contact Senior Vice President and Deputy General Counsel Mary Dunn or me at (202) 638-5777.

Sincerely,

Jeffrey Bloch
Senior Assistant General Counsel