National Association of Federal Credit Unions
3138 10th Street North • Arlington, VA 22201-2149
(703) 522-4770 • (800) 336-4644 • Fax (703) 524-1082
www.nafcu.org • nafcu@nafcu.org

September 18, 2006

Mary F. Rupp
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314

RE: Comments on Proposed Part 717, Identity Theft Red Flags

Dear Ms. Rupp:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association that exclusively represents the interests of our nation's federal credit unions (FCUs), I am responding to the request for public comment on a proposed rulemaking for implementation of identity theft red flags and address discrepancies under the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The proposed rulemaking has been jointly issued by the National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and Federal Trade Commission (FTC) (collectively, the Agencies).

The proposal, which would implement sections 114 and 315 of the FACT Act, would require each financial institution and creditor to have a risk-based written Identity Theft Prevention Program (Program) containing reasonable policies and procedures to address the risk of identity theft. The joint proposed rule also includes guidelines for financial institutions and creditors identifying patterns, practices, and specific forms of activity that indicate possible identity theft. It would also require credit and debit card issuers to establish reasonable policies and procedures for assessing the validity of a change of address request under certain circumstances. Additionally, users of consumer reports would be required to develop policies and procedures for handling notices of address discrepancies from a consumer reporting agency.

Identity theft continues to be a major threat to and a significant concern for American consumers. Identity theft costs time and money for financial institutions and may create significant risks to safety and soundness. Even worse, such fraud wreaks havoc on its victims by destroying credit histories, violating financial privacy, and ruining good names. NAFCU believes that credit unions should be vigilant and proactive in helping to protect their members

from this serious financial crime; as such, we generally support the proposed rule. However, NAFCU would like to take the opportunity to submit the following comments.

Red Flag Regulations

The proposed Red Flag Regulations require each institution or creditor to implement a written Program appropriate to its size, complexity, and scope of activities. The Program would be based upon the risk assessment of the institution and include controls designed to address the risk of identity theft to consumers and to the safety and soundness of the institution.

NAFCU generally supports the proposed Program requirements. The risk-based approach adopted by the Agencies will allow institutions greater flexibility in implementing a Program appropriate to its own risk profile. This risk-based approach will also allow institutions to more easily address evolving identity theft risks.

NAFCU, however, would like to encourage the Agencies to also operate a flexible and risk-based examination program. Indeed, rather than applying a strict set of compliance standards, examiners should be fully cognizant of each institution's individual risk assessment.

Red Flags Definition

Under the Agencies' proposal, the term "Red Flags" is defined broadly to incorporate precursors to identity theft which indicate the possible *risk*, not merely the possible *existence*, of identity theft. NAFCU supports the inclusion of early warning signals in the red flag definition. Earlier detection of potential risks increases the likelihood that identity theft can be thwarted; thus, the inclusion of precursors to identity theft as red flags will allow institutions to be more proactive in preventing the occurrence of identity theft.

Oversight of Third-Party Service Providers

The proposal would require that institutions and creditors engaging a third-party service provider to perform any covered activity take appropriate steps to ensure that the activity is conducted in compliance with the Red Flag Regulations. The proposal would also allow a service provider that provides services to multiple institutions to apply its own Program so long as the program complies with the Red Flag Regulations; the service provider would not be required to comply with the particular Program of each institution to which it provides services.

NAFCU agrees that service providers should be permitted to implement their own Programs as long as they comply with the Red Flag Regulations. It would be both inefficient and costly to require service providers to comply with the individual program of each institution to whom it is providing services. The increase in compliance costs to the service provider would eventually be passed on to institutions receiving services, and ultimately, to consumers.

NAFCU, however, believes that the final rule should clearly indicate that each financial institution is ultimately responsible for complying with the standards set forth in the Red Flag

Regulations. Because institutions and creditors would be obligated to exercise appropriate due diligence to ensure that third-party service providers are compliant with the Red Flag Regulations, NAFCU believes that it is necessary to clarify the Agencies' expectations for service provider arrangements in the final regulation. Additionally, NAFCU does not believe that financial institutions should be required to undertake costly independent testing of their servicers' identity theft programs to ensure compliance with the regulations. We recommend that the final rule clarify that that independent auditing of third-party Programs is not necessary.

Red Flag Guidelines: Appendix J

Proposed Appendix J lists Red Flags that could be relevant to detecting a possible risk of identity theft. Under the proposed Red Flag Regulations each financial institution and creditor would have flexibility to develop policies and procedures to identify which Red Flags in Appendix J are relevant to detecting the possible risk of identity theft.

NAFCU generally supports the use of guidelines that provide a significant degree of flexibility to allow institutions to adapt the requirements to their own individual needs and circumstances. As such, NAFCU believes that the Red Flags enumerated in proposed Appendix J are appropriate.

Account Inactive for a "Reasonably Lengthy Period of Time"

Section 114 of the FACT Act directs the Agencies to consider whether to include reasonable guidelines for notifying the consumer when a transaction occurs in connection with a consumer's credit or deposit account that has been inactive for "two years." The Agencies believe that the two-year limit may not be an accurate indicator of identity theft; therefore, a more flexible Red Flag on inactive accounts has been included in proposed Appendix J. Specifically, the appendix lists as a Red Flag the use of an account that has been inactive for a "reasonably lengthy period of time." NAFCU supports the adoption of this more flexible approach.

Special Rules for Card Issuers

Assessing the Validity of a Change of Address Request

The proposal would also require credit and debit card issuers to establish reasonable policies and procedures for assessing the validity of a change of address request under certain circumstances. The Agencies have requested comment on whether the final rule should elaborate further on the means that a card issuer must use to assess the validity of a request for a change of address.

NAFCU believes that some further elaboration might be helpful. While card issuers should be afforded a great deal of flexibility in verifying address change requests, some illustrative examples may be beneficial for some credit unions.

FCRA Definitions

The Agencies have also requested comment on whether the regulations implementing section 315 of the FACT Act should define additional terms that are already defined in the FCRA, for example "card issuer," "credit card," and "debit card."

For consistency, NAFCU recommends that the final regulation include the established definitions for these additional terms. Incorporating the FCRA definitions will help to avoid confusion and thus, aid compliance. At a minimum, NAFCU suggests that the final rule include a cross-reference to the statutory definitions.

Address Discrepancies

Under the proposal, users of consumer reports would also be required to develop policies and procedures for handling notices of address discrepancies from a consumer reporting agency. The proposed rule provides a list of illustrative measures that a user may employ to reasonably confirm the accuracy of a consumer's address. NAFCU believes that these illustrations are sufficient and further elaboration is not necessary

Timing

The proposed rule requires a user to furnish the consumer's address that it has reasonably confirmed to the credit reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer. However, where a consumer report is requested for an existing customer, the user would furnish this information for the reporting period in which the user has reasonably confirmed the accuracy of the address. Thus, the proposed timing provision for newly established relationships may not allow users to take full advantage of the flexibility in the timing for verification of identity under the customer identification program (CIP) rules. Indeed, a user employing CIP rules will have to both establish a continuing relationship and a reasonable belief that it knows the consumer's identity during the same reporting period. The Agencies have requested comment on whether this timing requirement is appropriate.

NAFCU believes that the proposed timing requirement for newly established relationships could be problematic for credit report users employing CIP rules. Most institutions report to credit reporting agencies on a monthly basis; in certain cases it may be difficult to verify a new customer or member within 30 days. For example, it can often take some time to gather the appropriate verification information for non-citizens or other individuals whose identities are verified through nondocumentary methods. Accordingly, NAFCU suggests that the timing requirement for newly established relationships be revised to provide the same flexibility that is afforded under the CIP rules. Alternatively, NAFCU recommends that the Agencies carve out an exception that would provide users employing CIP rules additional time to verify new customers so long as the process for identifying the individual's identity has been commenced during the same reporting period.

Additional Comments

Effective Date

NAFCU encourages the Agencies to provide adequate time to ensure full and proper implementation of all necessary operational changes. In establishing a mandatory compliance deadline, sufficient time must be allowed for implementation of any technology enhancements that will be required to comply with the new Red Flag regulation and guidelines. NAFCU recommends that a minimum of 1 year from the date of publication in the *Federal Register* be provided to allow credit unions sufficient time to implement and test system changes.

Data Security

Additionally, a number of NAFCU member credit unions have raised concerns about the increasing level of responsibility being placed on financial institutions to prevent and mitigate identity theft and to bear the significant costs for fraud losses. NAFCU believes that the war against identity theft must be fought on several fronts and that there must be a coordinated effort to combat this crime. Accordingly, NAFCU strongly urges the Agencies to consult with Congress and other regulatory agencies in order to push for increased liability for merchants and other unregulated organizations that compromise consumer data security. NAFCU also encourages the Agencies to support any congressional efforts to strengthen criminal penalties against identity thieves.

NAFCU appreciates this opportunity to share its comments on this proposed rulemaking and would like to commend the Agencies in their efforts in combating this serious crime. Should you have any questions or require additional information please call me or Pamela Yu, NAFCU's Associate Director of Regulatory Affairs, at (703) 522-4770 or (800) 336-4644 ext. 218.

Sincerely,

Fred R. Becker, Jr.
President/CEO

FRB/py