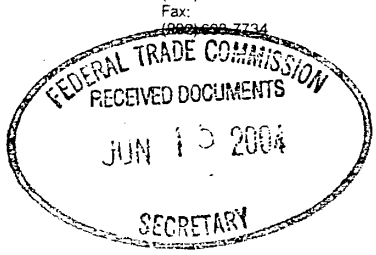
Credit Union
National Association, Inc.

**CUNA & Affiliates**
*A Member of the Credit Union System*

601 Pennsylvania Ave. NW, South Bldg.
Suite 600
Washington, D.C
20004-2601

Telephone:
(202) 638-5777
Fax:
(202) 638-7734

Web Site:
www.cuna.org




June 15, 2004

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

RE: FACTA Identity Theft Rule, Matter No. R411011

Dear Sir or Madam:

The Credit Union National Association (CUNA) is pleased to respond to the Federal Trade Commission's (FTC's) proposed rule that will provide definitions beyond those in the Fair and Accurate Credit Transactions (FACT) Act for "identity theft," identity theft reports," and "appropriate proof of identity" and will set the duration of the "active duty alerts" at 12 months, which may be extended. By way of background, CUNA is the largest credit union trade association, representing more than 90% of our nation's nearly 9,800 state and federal credit unions. The following comments were developed by CUNA with input from credit unions, credit union leagues, and CUNA's Consumer Protection Subcommittee, chaired by Kris Mecham, CEO of Deseret First Credit Union, Salt Lake City, Utah.

**Summary of CUNA's Position**

- The term "identity theft" should include attempted identity theft and the element that the person's identifying information has been used without lawful authority and without the person's knowledge.
- The FTC affidavit should be included in the "identity theft report," along with the law enforcement report. The affidavit will provide more specific information, which will facilitate compliance with the requirements regarding the filing of these reports. We also recognize that the process may be abused by consumers who file identity theft reports as a means to block unfavorable information on a credit report or for other fraudulent means. To alleviate these concerns, we would urge that efforts be undertaken to prevent this, such as encouraging law enforcement to refrain from making blank law enforcement reports readily accessible for consumers to use.

- Military personnel who are on active duty or assigned to service away from their usual duty station may request an "active duty alert" on their credit reports, which will require creditors using these reports to use reasonable means to determine the identity of the consumer. We believe military personnel should have the ability to tailor the length of the active duty alert to accommodate their personal circumstances.
- The FACT Act requires the FTC to determine the "appropriate proof of identity" when placing or removing an "active duty alert," "initial fraud alert" (which lasts for at least 90 days), or "extended fraud alert" (which lasts for seven years). The appropriate proof of identity is also required when a consumer requests that information be blocked from a credit report or requests that the Social Security number be truncated on a credit file. The examples in the proposed rule provide helpful guidance, and such methods of identification already appear to be standard within the credit union movement.

**Discussion**

The FACT Act gives victims of identity theft certain rights and creates requirements that creditors and others must follow to reduce the occurrence of this crime. With regard to the definition of "identity theft," the FTC has requested comment on whether the term should include attempted identity theft, the element that the person's identifying information has been used without lawful authority, and whether the term should also include information used without the person's knowledge.

We believe the term "identity theft" should incorporate these elements, including use without the person's knowledge, as well as include attempted identity theft. Without the requirement regarding the person's knowledge, there may be confusion as to the meaning of "without lawful authority," such as whether this would include information used unlawfully, but with the person's permission, such as schemes in which the "victim" works with another person to perpetrate fraud. Eliminating this possible confusion should help the FTC achieve the goal of preventing individuals from conspiring with others to obtain goods and services without paying for them and then claiming the rights available under the FACT Act.

Our only concern here is that adding this provision should not interfere with a creditor's right to use such information for lawful purposes, without the consumer's permission, for purposes of collecting a debt. One example would be skip-tracing activities. We urge the FTC to clarify that these would be permissible activities.

The FTC has requested comment on whether the phrase "identifying information" should have the same meaning as "means of identification" as used in the United States Criminal Code. We generally agree with this approach but request that the term refer to information identifying a person, rather than an individual. This

will be consistent with the definition of identity theft, which refers to a "person," and may provide additional protections for those individuals having credit relationships with businesses or other "persons," as defined in the Fair Credit Reporting Act.

Under the FACT Act, an "identity theft report" is filed to mitigate identity theft. The report may be filed to obtain an extended fraud alert, which is placed in the consumer's credit file for seven years and requires users of the file to contact the consumer to verify identity before extending credit, or filed in order to block information from the consumer's credit report. The proposed rule will expand the definition of "identity theft report" to require that allegations of identity theft include as much specificity as possible.

We believe that the FTC affidavit should also be required, along with the law enforcement report. The affidavit will provide more specific information, which will facilitate compliance with the expanded definition, especially in those jurisdictions in which the law enforcement report may only include check-off boxes with a request for a brief explanation of the incident.

We recognize that the process may be abused when consumers file reports as a means to block unfavorable information on a credit report or for other fraudulent means. To alleviate these concerns, we would urge that efforts be undertaken to encourage law enforcement to refrain from making blank law enforcement reports readily accessible for consumers to use. One example could be to limit the ability of consumers to download such reports from the Internet that they could then complete and file with law enforcement officials.

We agree with the FTC that it seems reasonable that levying criminal penalties will help to deter people from filing false reports, although using automated systems to generate reports may prove to be a less effective deterrent to identity theft than an "in-person" filing. However, we believe the single greatest weapon against identity theft will continue to be the ability of information furnishers and consumers reporting agencies to ask the appropriate questions and demand the appropriate information to resolve questions of fact. We believe that information furnishers and consumer reporting agencies have the expertise and experience to gather the appropriate information to determine whether a crime has been or is being committed and should be afforded the broadest regulatory latitude to conduct investigations.

The FTC has proposed that creditors and credit bureaus be allowed to request additional documentation within five days after receiving the report. This time frame may not be sufficient for credit unions to assess these identity theft claims.

Military personnel who are on active duty or assigned to service away from their usual duty station may request an "active duty alert" on their credit reports, which will require creditors using these reports to use reasonable means to determine

the identity of the consumer. Under the FACT Act, the duration of the active duty alert is at least 12 months, but the FTC has the authority to extend the time period. The proposed rule will not extend the time period, although active duty personnel may place another 12-month alert after the first alert expires.

We believe military personnel should have the ability to tailor the length of the active duty alert to fit their personal circumstances. The length of service away from the usual duty station may vary and be longer than one year. If the length of service is one year, this still may not provide military personnel sufficient time to extend the alert prior to expiration, especially if there is a training period prior to the one-year deployment. It is also possible that personnel may be too distracted or not able to easily extend their alert after the one-year period if they are still away from their usual duty station. For this reason, we believe military personnel should be able to request that the initial duty alert be the same duration as the anticipated length of service in those situations in which the length of service will be longer than one year. Another alternative would be to allow military personnel to place the alert for a period of time up to 24 months.

Our concern with regard to active duty alerts is that military personnel often provide their spouse or other close relative or friend with a power of attorney to act on their behalf, including credit transactions, while they are away from home. We urge the FTC to review this issue to ensure that active duty alerts do not interfere with these powers of attorney.

The FACT Act requires the FTC to determine the "appropriate proof of identity" when placing or removing an "active duty alert," "initial fraud alert" (which lasts for at least 90 days), or "extended fraud alert" (which lasts for seven years). The appropriate proof of identity is also required when a consumer requests that information be blocked from a credit report or requests that the Social Security number be truncated on a credit file.

Examples of such proof may include identification information of the victim, such as full name, previously used names, full address, Social Security number, and date of birth. This may also include additional proof, such as copies of government issued identification documents, utility bills, and other authentication methods.

We believe the definition of "appropriate proof of identity," as proposed, provides the appropriate regulatory latitude to information furnishers and consumer reporting agencies as they conduct their investigations. The examples included provide helpful guidance and such methods of identification already appear to be standard within the credit union movement. If managed properly, we believe this system will work well.

We agree with the FTC that the two greatest risks associated with misidentifying a consumer are a "mix-up" of consumer files and cases in which a person might make a request without the "real" consumer's knowledge. The first may require

only a small amount of additional information and may be resolved in a phone call while the second may require substantially more inquiry (and information) and require the involvement of law enforcement agencies.

Thank you for the opportunity to comment on the proposed rule that will provide definitions beyond those in the FACT Act for "identity theft," identity theft reports," and "appropriate proof of identity" and will also set the duration of the "active duty alerts" at 12 months. If you have questions about our comments, please contact Associate General Counsel Mary Dunn or me at (202) 638-5777.

Sincerely,

Jeffrey Bloch
Assistant General Counsel