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

To Whom It May Concern:

This comment letter is submitted on behalf of the Consumer Bankers Association ("CBA") in response to the proposed rule ("Proposed Rule") issued by the Federal Trade Commission ("FTC") regarding the definitions of "identity theft" and "identity theft alert," as well as the duration of an active duty alert. CBA is the recognized voice on retail banking issues in the nation's capital. Member institutions are the leaders in consumer financial services, including auto finance, home equity lending, card products, education loans, small business services, community development, investments, deposits and delivery. CBA was founded in 1919 and provides leadership, education, research and federal representation on retail banking issues such as privacy, fair lending, and consumer protection legislation/regulation. CBA members include most of the nation's largest bank holding companies as well as regional and super community banks that collectively hold two-thirds of the industry's total assets.

We thank the FTC for the opportunity to comment on the Proposed Rule.

Definition of "Identity Theft" and "Identifying Information"

Congress recently passed the Fair and Accurate Credit Transactions Act ("FACT Act") to, among other things, provide significant new protections to victims of identity theft. Not surprisingly, many of these protections are based on activities defined as "identity theft." For example, many types of financial institutions will be required to adopt "red flags" programs related to identity theft. Consumers who are victims of identity theft will be able to use new rights to correct any damage in their credit histories resulting from identity theft. Victims of identity theft will also have the opportunity to place extended fraud alerts in their credit files.

The Fair Credit Reporting Act ("FCRA"), as amended by the FACT Act, defines "identity theft" to mean "a fraud committed using the identifying information of another person, subject to such further definition as the [FTC] may prescribe." Congress focused the definition on consumers

who have suffered a fraud through misuse of their identity, but the statute gives the FTC the flexibility to amend this definition as the concept of identity theft continues to evolve. The Proposed Rule defines "identity theft" to mean "a fraud committed or attempted using the identifying information of another person without lawful authority."

Attempted Identity Theft

The Proposed Rule would include identity thefts that have been avoided, or attempted identity thefts, as "identity theft" for purposes of the FCRA. An impact of this greatly expanded definition of identity theft would be that financial institutions would need to dedicate scarce resources to comply with the requirements pertaining to the "red flags" programs and identity theft reports. With respect to identity theft prevention and mitigation, CBA believes that its members should focus on demonstrated weaknesses in preventing identity theft and on mitigating the harm to actual victims of identity theft. Therefore, we are concerned that the Proposed Rule would force our members to divert resources from preventing identity theft, and assisting victims, in order to assist those who have avoided the harms of identity theft. We do not believe that the FTC intends for this result, and urge the definition of "identity theft" to apply only to those people who have had their identities stolen.

In the Supplementary Information, the FTC implies that an expanded definition of "identity theft" is necessary in order to allow consumers to remove fraudulent inquiries from their credit files. Although the FACT Act provides new a mechanism under Section 605B of the FCRA to block the reporting of the inquiry, the consumer has other viable alternatives to remove such inquiries by using the dispute process under Section 611 of the FCRA. We do not believe that the extremely modest benefits provided in Section 605B in the context of removing false inquiries[1] justifies the harm associated with an unnecessarily broad definition of identity theft.

The FTC also indicates that an expanded definition of "identity theft" would be helpful for consumers "who have learned of attempts by an identity thief and want to…place an 'initial fraud alert'" in their consumer files. While CBA believes it would be appropriate for a consumer to place an initial alert in a consumer's credit file if he or she is the subject of an attempted identity theft, it is not necessary to expand the definition of "identity theft" in order to achieve this goal. Specifically, the FCRA permits a consumer who "asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime" to place an initial alert in his or her file—there is no requirement that the consumer be a victim of identity theft. Therefore, an expanded definition of "identity theft" is not necessary to achieve the FTC's policy goal in this respect.

If the FTC retains attempted identity theft as part of the definition of "identity theft," we urge the FTC to provide clear guidance as to what "attempted" identity theft means. For example, using the FTC's justification for its inclusion, attempted identity theft should be limited to the types of activities that would result in fraudulent inquiries on a consumer, such as a fraudulent application for credit. On the other hand, it would not serve the FTC's stated objectives to include a foiled pretexting call, for example, as an attempted identity theft.

[1] The presence of inquiries generally has a very minor impact on a consumer's credit score.

Using the Identifying Information of Another Person

The Proposed Rule would require that "identity theft" involve the use of the "identifying information" of another person. We believe that the natural predicate for "identity theft" would involve the use of information that allows a criminal to assume a victim's identity. The FTC defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual."

We believe that the definition of "identity theft" should reflect situations where a victim's identity is assumed by the criminal. In contrast, we do not believe that any fraud relating to a consumer's name or account should be deemed to be *per se* "identity theft." Such a broad definition would require a financial institution to diffuse its efforts to assist those whose identities have been stolen in order to assist other victims of fraud in ways that are not appropriate to those types of fraud. For example, the Truth in Lending Act and the Electronic Fund Transfer Act provide specific and effective remedies consumers may pursue in connection with the unauthorized use of their credit or debit cards. We do not believe that Congress intended to address these issues through the FACT Act, nor do we believe that Congress intended to place equal priorities with respect to a consumer who has suffered a one-time unauthorized use of an account and a consumer who has had his or her identity hijacked.

Therefore, we strongly urge the FTC to reconsider what types of information would qualify as "identifying information." The types of information involved should be of the type that allows a criminal to masquerade as the victim with respect to new accounts or altering existing accounts. Simple misuse of an existing account should not rise to the level of becoming an "identity theft."

We also note that the definition of "identifying information" would appear to be limited to a name or a number. However, the examples of information that would be "identifying information" under the Proposed Rule include things such as a fingerprint or voice print. We urge the FTC to either revise the definition such that a fingerprint could be included, or to revise the examples to ensure that they are consistent with the definition of the term. For example, the definition could simply say: "The term 'identifying information' means any information that may be used to identify a specific individual, including…"

Without Lawful Authority

The Proposed Rule would require that an "identity theft" be a "fraud committed…without lawful authority." The FTC states that "[a]dding 'without lawful authority' [to the definition] prevents individuals from colluding with each other to obtain goods or services without paying for them, and then" attempting to allege that it is the result of identity theft. CBA applauds the FTC for addressing this important issue. We do not believe that consumers who benefit from a transaction should be able to claim that the transaction is the result of identity theft. Therefore, we urge that this concept be retained. However, we also ask the FTC to clarify this issue in the Final Rule. In particular, as the definition is drafted, it is not clear whether the modifier "without lawful authority" would achieve the FTC's objective because a fraud is already generally an act committed without lawful authority. Rather, it may be useful to state that "identity theft" does not include frauds committed in which the "victim" colluded with the perpetrator, from which

the "victim" obtained a benefit (such as an interest in, or possession of, the goods or services purchased), or where the "victim" voluntarily provided the perpetrator access to the account.

Definition of "Identity Theft Report"

The FCRA provides a victim of identity theft the ability to block the false information resulting from the identity theft from harming their credit histories. For example, a victim can submit an identity theft report, in addition to other things, to a consumer reporting agency to block information that resulted from identity theft. The victim can also use a similar process to block an entity from furnishing such information. Congress deemed the need to provide identity theft victims with such powerful tools as necessary to mitigate the effects of identity theft. CBA agrees with this approach as a meaningful tool to help identity theft victims and to preserve the integrity of consumer report data.

Congress was also aware that an "identity theft report" could be misused by those seeking to abuse the system and block the reporting of negative, but accurate, information. Therefore, Congress provided for specific minimum requirements with respect to identity theft reports in order to lessen the likelihood of fraud associated with misuse of the reports. Therefore, the FCRA defines an "identity theft report" to be, "at a minimum," a report:

> "(A) that alleges an identity theft;
> "(B) that is a copy of an official, valid report filed by the consumer with an appropriate…law enforcement agency…or such other government agency deemed appropriate by the [FTC]; and
> "(C) the filing of which subjects the person filing the report to criminal penalties relating to the filing of false information…."

As part of the Supplementary Information, the FTC recognizes the benefits of an identity theft report, but also notes that "it could provide a powerful tool for misuse, allowing persons to engage in illegal activities in an effort to remove or block accurate, but negative, information in their consumer reports." The FTC further asserts that it "is concerned whether [the] safeguards [in the FCRA] provide sufficient protection from misuse." Therefore, "[t]o address these concerns," the FTC has included two additional elements to the definition of an identity theft report. First, the report must allege identity theft "with as much specificity as the consumer can provide."[2] Second, the consumer reporting agency or the furnisher receiving the report is permitted a limited opportunity to request additional information.

Although we believe the FTC has provided for some beneficial concepts in the definition of an "identity theft report," we do not believe that they will address the concerns identified by the FTC. In this regard, CBA does not believe that a requirement to provide details about the identity theft will deter credit repair clinics and other fraudsters from filing identity theft reports for fraudulent purposes. If the person is willing to commit fraud by lying to a bank or to a consumer reporting agency, that person is likely to have a story to back it up.

[2] We believe this concept should be retained and that it should also require the consumer to identify the specific information that he or she wishes to block.

Filing the Report with an Appropriate Agency

We believe it would be more appropriate for the FTC to focus on the need for the report to be a document that is filed with an "appropriate" law enforcement agency. Although this concept was omitted from the Proposed Rule, the statute requires that the document be filed with an appropriate law enforcement agency. This requirement is meant to deter people from filing false reports with far away law enforcement agencies with no interest or jurisdiction to investigate the crime. For example, the statute would appear to prohibit the filing of an identity theft report with the Federal Communications Commission ("FCC"), because an agency charged with enforcing several different laws unrelated to identity theft would clearly not be an appropriate recipient of a report alleging identity theft. Not only can the FCC do very little about investigating the identity theft, but the FCC is unlikely to spend a lot of resources to determine whether the consumer has lied in the report. However, by requiring the report to be filed with a law enforcement agency with an interest in the veracity of the document, such as an agency that can investigate the crime, Congress provided a significant deterrent to those seeking to abuse the system.

The Supplementary Information appears to add credence to this concern. The FTC identifies its own identity theft reporting system as an example that "illustrates the possibility for abuse" if it were to be used as a foundation for an identity theft report. In this regard, the FTC states that the system "is not designed to vouch for the truth of each individual complaint. It is simply designed to provide a central collection point for identity theft data. Victims who have filed complaints with the [FTC] have done so…with no guarantee of obtaining any immediate, direct benefit such as the investigation of their cases."[3] For the reasons the FTC has provided, CBA agrees that the FTC would not be an appropriate law enforcement agency with which to file an allegation of identity theft for purposes of the allegation becoming an "identity theft report." We believe that if an effective deterrent to fraudulent identity theft reports is to be provided, the definition of an "identity theft report" must include the notion that the report be filed with an appropriate law enforcement agency. Not only will this deter fraud, but it will also benefit consumers by putting them in contact with an agency that can investigate the crimes. In light of the many law enforcement options available to the consumer, which could include the local police department, the Federal Bureau of Investigation, or the U.S. Postal Inspection Service, we do not believe such a requirement poses a legitimate hindrance to identity theft victims.

Prohibiting Credit Repair Clinics and Others From Filing

We believe an important corollary to the requirement that the identity theft report be filed with an appropriate law enforcement agency is that the report must be filed by the consumer, and not by another entity. CBA is concerned that credit repair clinics and other unscrupulous individuals should not be permitted to file identity theft reports on consumers' behalf. Although this improvement would not be sufficient on its own to significantly deter abuse, we do believe that it would be an important amendment in addition to our other suggestions.

Obtaining Additional Information

[3] Given this obvious weakness, we are concerned that the FTC appears to believe that a complaint filed with the FTC would meet the statutory definition of an "identity theft report" (*i.e.*, that it was filed with an "appropriate" law enforcement agency).

The Proposed Rule would allow a furnisher or a consumer reporting agency to obtain additional information from the victim in connection with the submission of an identity theft report. Specifically, the furnisher or agency may request additional information "for the purpose of determining the validity of the alleged identity theft" not later than five business days after the receipt of the report. We commend the FTC for allowing furnishers and consumer reporting agencies to request additional information. However, we are concerned that this opportunity is limited to a single request for limited purposes. A furnisher or agency should be permitted to make the requests necessary for legitimate purposes, such as to ensure the appropriate information is blocked or to investigate the crime itself. Furthermore we do not believe that five business days is sufficient for a furnisher to determine whether it needs additional information. We believe that 30 days would be more appropriate.

Duration of Active Duty Alerts

Military personnel who meet the definition of an "active duty military consumer" may request that an active duty alert be placed in their credit files. This alert is intended to notify users of the consumer's consumer report that the consumer is on active duty and to take note of potentially fraudulent activities. The statute requires that an active duty alert remain in a consumer's file for at least twelve months, although this timeframe may be extended by the FTC.

The Proposed Rule would not amend the twelve-month duration for active duty alerts. CBA agrees that an active duty alert should last for twelve months. This would appear to suffice for most active duty military consumers. For those who need additional time, a subsequent active duty alert is available. Therefore, the twelve months established by Congress appears to be a reasonable period of time for an active duty alert to remain in a consumer's credit file.

Appropriate Proof of Identity

The FACT Act requires the FTC to determine what constitutes "appropriate proof of identity" for purposes of Sections 605A, 605B, and 609(a)(1) of the FCRA. The Proposed Rule requires consumer reporting agencies to "develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity." We commend the FTC for determining that the consumer reporting agencies are in the best position to determine what should suffice as "appropriate proof of identity" in these circumstances. Like the FTC, we believe that the consumer reporting agencies are best equipped to evaluate the risks of misidentifying the consumer as well as the types of information that would be necessary to identify the consumer properly. Therefore, we urge the FTC retain this approach in the Final Rule.

Once again, CBA thanks the FTC for the opportunity to comment on the Proposed Rule. If you have any questions in connection with our comments, or if we may provide any additional information, please do not hesitate to contact me at msullivan@cbanet.org or 703-276-3874.

Very Truly Yours,

Marcia Z. Sullivan
Vice President and Director, Government Relations