













919 18th Street, NW
Suite 300
Washington, DC 20006

Jeffrey A. Tassey
Executive Director
Phone: 202-464-8815

COALITION TO IMPLEMENT THE FACT ACT

June 14, 2004

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

Re: FACT Identity Theft Rule, Matter No. R411011

To Whom It May Concern,

This comment letter is submitted on behalf of the Coalition to Implement the FACT Act in response to the Federal Trade Commission's ("FTC") proposed rule pertaining to identity theft definitions, the duration of active duty alerts, and the definition of "appropriate proof of identity" under the Fair Credit Reporting Act ("FCRA") ("Proposed Rule"). The Coalition represents a full range of trade associations and companies that furnish and use consumer information, as well as those who collect and disclose such information. We appreciate the opportunity to provide our comments on the Proposed Rule.

Definition of "Identity Theft"

The FCRA, as amended by the Fair and Accurate Credit Transactions Act ("FACT Act"), includes significant consumer protections related to identity theft. For example, a victim alleging an identity theft has the opportunity to obtain an "identity theft report" which can be used to rehabilitate credit files damaged as a result of the identity theft. The identity theft report can also be used to insert an extended fraud alert on the victim's credit file, requiring users of the victim's consumer report to take additional precautions when transacting with the victim (or an individual claiming to be the victim) in certain circumstances. An identity theft victim can also contact a business entity that transacted with the identity thief in order to obtain information to investigate the crime. Financial institutions and creditors will also be required to adopt reasonable policies and procedures regarding identity theft to protect account holders and customers.

The FCRA defines "identity theft" as "a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation." In light of the fact that the term "identity theft" is central to many of the new provisions added by the FACT Act, it is critically important for the FTC to provide an appropriate definition of "identity theft."

The Proposed Rule defines "identity theft" to mean "a fraud committed or attempted using the identifying information of another person without lawful authority." We commend the FTC for defining the term in a manner that is largely consistent with the congressional intent as evidenced by the statutory language. We also applaud the Commission for modifying the definition to include the words "without lawful authority" in an effort to prevent individuals from colluding with each other to obtain goods or services without paying for them and then trying to allege that the transaction resulted from identity theft. The Coalition asks the FTC to include this clarification in the definition of "identity theft" as it appears in the final rule ("Final Rule") itself. We believe that such language in the Final Rule would be useful in clarifying that a consumer who benefits from a transaction, or who colludes with another as part of the transaction, cannot attempt to abuse the system by claiming that it was part of an identity theft.

The Coalition is concerned, however, that the Proposed Rule defines "identity theft" to include situations where identity theft was actually prevented—*i.e.*, when the identity theft was only attempted, but not successful. We believe that such a broad definition of "identity theft" would require private and public sector entities to dedicate scarce resources to individuals who have not been victimized by identity theft at the expense of those who are victims of identity theft. For example, if the definition is not modified, law enforcement agencies will undoubtedly need to dedicate scarce resources to individuals seeking to file "identity theft reports" that pertain to situations where identity theft was actually averted. Financial institutions and others will need to dedicate scarce resources toward policies and procedures, or responses to consumers, pertaining to identity thefts that they have already been able to thwart. These resources would be better spent helping existing victims or preventing future attempts at identity theft. Therefore, we believe that the definition of "identity theft" should focus on actual transactions involving identity theft, as opposed to attempts.

The FTC notes that a broader definition may be appropriate because "[a]lthough identity thieves do not always succeed in opening new accounts, their attempts may be recorded as inquiries on victims' consumer reports. These inquiries may have an adverse affect on their credit scores, therefore, victims should be entitled to take advantage of the [FACT] Act to have these inquiries removed." The Coalition agrees that consumers should have the ability to remove bogus inquiries from their credit files. However, it does not necessarily follow that consumers must take advantage of the information blocking tools provided in the FACT Act. Indeed, consumers have the ability to remove inquiries from their files using the dispute process in Section 611 of the FCRA or by contacting the furnisher of such information under Section 623(a)(1)(B) of the FCRA (if the furnisher specifies an appropriate address, which many do). Although the information blocking provisions in the FACT Act provide a powerful tool to consumers in addition to those that were already in the FCRA, we do not believe that the definition of "identity theft," and therefore the resources dedicated to identity theft victims, should be diluted in order

to allow inquiries to be removed from credit files in yet another manner.

The FTC also implies that an expanded definition of "identity theft" is appropriate because "victims who have learned of attempts by an identity thief and want to reduce the likelihood that the identity thief will succeed in opening new accounts, may want to place an 'initial fraud alert' on their consumer reports." However, a consumer need not be a victim of identity theft in order to place an initial fraud alert in his or her credit file. Rather, the consumer must only "assert[] in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime." We believe that a consumer who has recently been a victim of attempted identity theft could make such an assertion, regardless of how "identity theft" is defined.

The Coalition also requests that the FTC review its definition of "identifying information." Under the Proposed Rule, "identifying information" means "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." As a primary matter, we believe that the definition must be sufficient so that it encompasses only those types of fraud which result in the theft of a person's identity. In other words, the information used must be of a type that allows the criminal to actually assume the victim's identity. For example, account fraud, while a serious crime, would not rise to the level of identity theft since the criminal is only accessing an account fraudulently—not obtaining the ability to actually assume the accountholder's identity. Not only are there already provisions in existing law, such as under the Truth in Lending Act and the Electronic Fund Transfer Act, to protect consumers who are victims of crimes such as account fraud, but we do not believe it would benefit victims of true identity theft to dilute industry's efforts by giving victims of less debilitating crimes equal priority as identity theft victims.

We also note that the definition of "identifying information" appears to have an inconsistency. In particular, the definition limits the scope of the term to a consumer's name or number. However, examples of identifying information include a fingerprint and a voice print. We ask the FTC to provide clarity with respect to whether "identifying information" could include more than a name or number in the Final Rule.

Definition of Identity Theft Report

Congress provided consumers with exceptionally useful mechanisms to restore credit histories that have been damaged by identity thieves. For example, a consumer can block a consumer reporting agency from reporting a tradeline resulting from identity theft if the consumer provides the agency with an "identity theft report" (among other things). The consumer can also block a furnisher from providing data resulting from an identity theft to a consumer reporting agency if the consumer provides the furnisher with an "identity theft report" at an address specified by the

furnisher. In essence, an "identity theft report" gives the consumer unprecedented ability to prevent data from being provided to users of consumer reports. The consumer benefits of these provisions are obvious. However, Congress also recognized that these provisions could be abused by individuals seeking to remove negative, but accurate, information from their credit files. Therefore, Congress provided for some protections against such fraud by making an identity theft report a document that, "at a minimum," is filed with an appropriate law enforcement agency, the filing of which subjects the person filing the report to criminal penalties for false statements if the report is false. Congress delegated additional authority to the FTC to define what is meant by an "identity theft report."

In the Proposed Rule, the FTC has added some requirements to the definition of an "identity theft alert" because the FTC "is concerned whether safeguards [against fraud] provide sufficient protection from misuse." The Proposed Rule defines an "identity theft report" to be a report:

- That alleges identity theft with as much specificity as possible;
- That is a copy of an official, valid report filed by the consumer with a federal, state, or local law enforcement agency;
- The filing of which subjects the person filing the report to criminal penalties relating to the filing of false information if the report is false; and
- That may include additional information or documentation that a furnisher or consumer reporting agency reasonably requests for the purpose of determining the validity of the identity theft, provided that the request is made no later than five business days after the report is received.

The two key additions to the definition require the consumer to allege identity theft "with as much specificity as possible" and allow the furnisher/consumer reporting agency to request additional information. The FTC believes that the revised definition is "balanced to prevent abuse of the credit reporting system, without creating road blocks to a victim's recovery process."

The Coalition is pleased that the FTC has provided opportunities for furnishers and consumer reporting agencies to receive as much information as possible in connection with an alleged identity theft. Because such information may be important in order to effectuate the consumer's request, we urge that the FTC retain these concepts in the Final Rule and specify that an "identity theft report" must include the specific information to be blocked. However, we do not believe that the concepts added by the FTC will provide sufficient road blocks to those seeking to abuse the system. In essence, if someone is willing to provide false information to

a furnisher or consumer reporting agency, it is reasonable to expect that person to be willing to provide a false story in connection with the report. Therefore, we do not believe that the Proposed Rule includes necessary safeguards to protect against abuse.

One critical safeguard available to the FTC is included in the statutory definition of an "identity theft report." In particular, Congress specified that an "identity theft report" is a report that, "at a minimum," is filed with an "appropriate" law enforcement agency. The Proposed Rule omits this critical requirement and we urge the FTC to reinsert this concept in the Final Rule as required by Congress. The Coalition believes that by requiring a person to file an identity theft report with an appropriate law enforcement agency (*i.e.*, one that has the jurisdiction to investigate the allegations in the report, the jurisdiction to take appropriate action, and the ability to take action against the individual if the report contains false information), Congress has provided a significant deterrent to those who may attempt to abuse the system. Although not a complete defense against fraud, a requirement to file the report with a law enforcement agency that can act upon the report, and take an interest in those persons who file false allegations, should deter many people who would like a low-risk method to eliminate negative, but accurate, information in their files.

The Coalition is pleased that the FTC has provided a good example of how an individual could abuse the system if a report could be filed with any law enforcement agency in the country, regardless of whether it is appropriate under the circumstances. In footnote 9 of the Supplementary Information, the FTC states that "the [FTC's] own identity theft complaint collection system...illustrates the possibility for abuse...The [FTC's] complaint system...is not designed to vouch for the truth of each individual complaint...Now under the [FACT] Act, a consumer could opt to use a copy of a complaint filed with the [FTC] as an 'identity theft report' because such a copy would technically meet the statutory definition." We do not believe that a report filed with the FTC would, in fact, meet the statutory definition of an "identity theft report" because, to use the FTC's own example, it is clearly not an "appropriate" law enforcement agency for these purposes. However, in light of the obvious potential for widespread abuse, we are concerned that a report filed with the FTC would meet the definition provided in the Proposed Rule.

We also request the FTC to clarify that an "identity theft report" is a report prepared and submitted by the consumer. In this regard, we believe that such reports should not be prepared by credit repair clinics or other unscrupulous individuals. Although this safeguard must be combined with the others we have suggested if it is to provide much of a safeguard, we believe it could be a useful protection against abusive activities involving credit repair clinics.

Regardless of the need to add additional safeguards to the definition of an "identity theft report," if the FTC retains the provision allowing furnishers and

consumer reporting agencies to request additional information, we urge the FTC to modify the provision to make it more workable. Specifically, we believe that a furnisher (especially smaller ones) may need more than five business days to request additional information from the consumer. The furnisher may need time to receive the report, process it, review its contents, and search its own files before it realizes that it needs additional information. We are also concerned that credit repair clinics may attempt to overwhelm furnishers with bogus identity theft reports and attempt to run out the clock with respect to the five-day period. Therefore, we believe it would be more appropriate to allow a request to be made within fourteen business days.

The Proposed Rule also limits the ability to request additional information only "for the purpose of determining the validity of the alleged identity theft." The Coalition believes that there are other legitimate reasons to request information from the consumer. For example, additional information may be needed to clarify the information to be blocked, to obtain additional details of the fraud, or to obtain the consumer's promise to cooperate with the investigation of the identity theft. These may not be related to the "validity" of the consumer's claim, but they are legitimate requests that should be permitted. We also urge the FTC to clarify that unless the consumer provides the information that is requested by the furnisher or consumer reporting agency, the report filed by the consumer will not be deemed to be an "identity theft report" for purposes of the FCRA.

Duration of an Active Duty Alert

Military personnel who meet the definition of an "active duty military consumer" may request that an active duty military alert be placed in their credit files. This provides such military personnel with important protections against possible identity theft while deployed. The FCRA provides that an active duty military alert has a duration of at least twelve months, although the FTC may provide for a longer duration.

The FTC has proposed that the duration of an active duty alert remain at twelve months. The FTC states that twelve months will cover adequately the time period for which the majority of service members will be deployed. For those who need additional time, the FTC correctly notes that such personnel can request a subsequent alert to be placed in their files. Therefore, we agree with the FTC's determination and urge that an active duty military alert have the duration of twelve months.

Definition of Appropriate Proof of Identity

The FACT Act directs the FTC to determine what constitutes "appropriate proof of identity" for purposes of Sections 605A (fraud alerts), 605B (tradeline blocking), and 609(a)(1) (Social Security number truncation) of the FCRA. It is criti-

cal that a consumer present "appropriate proof of identity" in connection with the activities under these sections in order to ensure that the consumer's request is matched with his file and to ensure that it is, in fact, the consumer and not an impostor making the request.

We applaud the FTC for determining that the consumer reporting agencies "are in the best position to assess" the risks associated with evaluating a consumer's proof of identity. The Proposed Rule requires consumer reporting agencies to "develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity for purposes of sections 605A, 605B, and 609(a)(1)" of the FCRA. We believe this is the proper approach, and that it should be retained in the Final Rule.

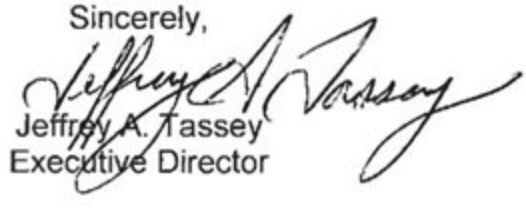
The Proposed Rule states that "[i]n developing these requirements" a consumer reporting agency must "ensure that the information is sufficient to enable the consumer reporting agency to match consumers with their files." We believe that the FTC's intent is to require a consumer reporting agency to obtain the types of information that would enable such a match—not that there must be a perfect match each and every time, which is an impossible standard. We ask the FTC to clarify this point.

Conclusion

The FACT Act amends the FCRA to provide a significant and appropriate increase in consumer protection relating to identity theft. To make these protections effective and to ensure that resources are allocated where they do the most good for consumers, while minimizing opportunities for abuse, the Coalition urges the FTC to include the definitional clarifications, refinements and modifications discussed above in relation to the terms "identity theft" and "identity theft report". Additionally, we endorse the FTC proposal as to the duration of a military alert and while we applaud the FTC approach regarding "appropriate proof of identity", it is critical that the accompanying standard for file matching receive clarification.

Thank you again for allowing the Coalition to comment on this issue. Please do not hesitate to contact me at 202 464 8815 if the Coalition can be of further assistance.

Sincerely,



Jeffrey A. Tassey
Executive Director