TransUnion

555 West Adams Street
Chicago, IL 60661
Tel 312 466 7730
Fax 312 466 7986
jblenke@transunion.com
www.transunion.com

John W. Blenke
Executive Vice President
General Counsel

June 15, 2004

The Federal Trade Commission
Office of the Secretary
Room 159-H (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 TransUnion LLC ("TransUnion") in response to the proposed rule issued by the Federal Trade Commission ("FTC") regarding the definition of certain terms in the Fair Credit Reporting Act ("FCRA") and the duration of an active duty alert ("Proposed Rule"). TransUnion is a Delaware limited liability company that employs approximately 3,600 people with operations on five continents and in 24 countries. TransUnion is a consumer reporting agency as such term is defined in the FCRA. We appreciate the opportunity to share our comments with the FTC as it prepares a final rule ("Final Rule").

Definition of "Identity Theft" and "Identifying Information"

The FCRA, as amended by the Fair and Accurate Credit Transactions Act ("FACT Act"), creates many new protections and rights for individuals who are victims of "identity theft." For example, a victim of an "identity theft" may obtain an identity theft report and mitigate damage to his or her credit file resulting from the identity theft. A victim may also contact any business entity to obtain information for purposes of documenting fraudulent transactions resulting from identity theft. Therefore, the definition of "identity theft" is important insofar as it outlines the scope of applicability for many of these new provisions.

Congress defined "identity theft" to mean "a fraud committed using the identifying information of another person, subject to such further definition as the [FTC] may prescribe." The Proposed Rule defines "identity theft" to mean "a fraud committed or attempted using the identifying information of another person without lawful authority." According to the FTC, it added "without lawful authority" to the statutory definition in order to prevent individuals from colluding with each other to obtain goods or services without paying for them, and then availing themselves of the rights provided under the FCRA to clear their credit records. We commend the FTC for excluding situations where the person obtains benefits from the alleged identity theft

from the definition of "identity theft." We ask the FTC to make this provision more clear in the text of the Final Rule, either through examples or in the definition itself.

In order to be an "identity theft," it must be a fraud committed using "the identifying information" of another person. The Proposed Rule defines "identifying information" to mean "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." The FTC has provided examples of such information in the Proposed Rule, including such things as voice prints or fingerprints. TransUnion is concerned that the examples provided by the FTC are not necessarily consistent with the plain language of the proposed definition. For example, "identifying information" is apparently limited to "any name or number." However, it is not clear how a voice print or fingerprint would be an example of a name or a number. Therefore, we urge the FTC to revise the examples to provide clarity with respect to what types of information will be deemed to be "identifying information."

Definition of "Identity Theft Report"

The FCRA includes new mechanisms for victims of identity theft to mitigate the damage to their credit histories. For example, a victim can provide an identity theft report, in addition to other information, to a consumer reporting agency and have the agency block the reporting of information resulting from the alleged identity theft. A victim can also provide an identity theft report to a data furnisher and block the furnisher from providing the information in question to a consumer reporting agency. An identity theft report is also required if the victim would like to add an extended fraud alert to his or her credit file at a nationwide consumer reporting agency.

In enacting the FACT Act, Congress recognized that an identity theft report provided victims with additional protections. But Congress also recognized that an identity theft report cannot be a document that could easily be fabricated by those seeking to abuse the system by blocking accurate, but negative, information. Therefore, Congress specified that certain requirements must be met before a document can be deemed to be an "identity theft report." Specifically, an "identity theft report" "has the meaning given that term by rule of the [FTC], and means, at a minimum, a report:"

- That alleges identity theft;
- That is a copy of an official, valid report filed by a consumer with an appropriate federal, state, or local law enforcement agency, or such other government agency deemed appropriate by the FTC; and
- The filing of which subjects the person filing the report to criminal penalties for false statements if information in the report is false.

The FTC has proposed a definition for "identity theft report" that is very similar to the statutory definition. However, the FTC states that it "is concerned whether these safeguards [in the statute] provide sufficient protection from misuse." Therefore, the Proposed Rule includes two additional elements to the definition of "identity theft report." First, the report must not only allege identity theft, but it must do so "with as much specificity as the consumer can provide." Second, consumer reporting agencies and furnishers will have the opportunity in certain

circumstances to request additional information from the alleged victim "for the purpose of determining the validity of the alleged identity theft."

TransUnion applauds the FTC for including provisions to ensure that an identity theft report contains as much information as possible. The concepts should be retained in the Final Rule. We do not believe, however, that these additional provisions in the Proposed Rule provide much deterrent to those seeking to file bogus documents and claim that they are identity theft reports. In particular, we expect that credit repair clinics and others seeking to manipulate accurate, but negative, information in a credit file will not have difficulty alleging identity theft with specificity and providing any additional (bogus) information that is requested by a consumer reporting agency or a furnisher.

If the FTC seeks to improve the safeguards related to an identity theft report, which we believe is critical if the integrity of consumer report data is to be preserved, it would be more appropriate for the FTC to opine on what it means to file an "official, valid" report with an "appropriate" law enforcement agency. It simply cannot be the case that an identity theft report is a document alleging identity theft that an individual files with any one of the thousands of law enforcement agencies in this country, regardless of the circumstances. For example, it would clearly not be appropriate to file a report alleging identity theft with the federal Food and Drug Administration (an agency charged with enforcing several laws). Rather, we believe Congress intended that the report be an official document filed with an *appropriate* law enforcement agency, such as one with the jurisdiction to investigate the alleged identity theft and enforce the law with respect to any violations. We believe that such a safeguard will deter many of those seeking to eliminate accurate, but negative, information from their credit files.

The FTC acknowledges the need for such a safeguard. The FTC states that its own identity theft collection complaint system illustrates the possibility for abuse if an "identity theft report" does not include the appropriate safeguards. In particular, according to the FTC, "[t]he [FTC's] complaint 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...Now under the [FCRA], 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."[1] The FTC has sufficiently detailed the issue to be resolved. However, we do not believe that simply requesting additional information from the alleged victim would address the weaknesses identified by the FTC. Nor would requiring the individual to have the document notarized, as is suggested in an example provided by the FTC.[2] Therefore, we strongly urge the FTC to require that an "identity theft report" be an "official" document filed with an "appropriate" law enforcement agency.

As mentioned above, we ask that the FTC retain the ability of consumer reporting agencies and furnishers to obtain additional information from identity theft victims. However,

---

[1] We note that such a report should not be considered to meet the statutory definition because it would not be filed with an "appropriate" law enforcement agency. However, it would appear to meet the definition provided in the Proposed Rule.

[2] Similar to the FTC's complaint system, a notary cannot necessarily vouch for the accuracy of the allegations in an identity theft report. A notary only signifies that the signatory has provided sufficient identification indicating that he or she is who he or she claims to be.

we believe that the request should not be limited only for purposes of determining the validity of the alleged identity theft. A consumer reporting agency may need additional information for a variety of other legitimate reasons, such as to ensure that the correct information is blocked or to further investigate the crime. We are also concerned that the request must be made within five business days. We believe that ten business days is more appropriate in light of the need to thoroughly review the information provided. TransUnion also requests that the FTC clarify that the information provided by the victim is not an "identity theft report" until the requested information has been provided.

Duration of an Active Duty Alert

Certain military personnel have the ability to include an active duty alert in their credit files. The FCRA establishes that an active duty alert must remain in the file for not less than twelve months (unless the consumer requests that it be removed sooner) "or such longer period as the [FTC] shall determine." The Proposed Rule would retain the twelve-month duration for active duty alerts.

TransUnion requests the FTC to retain the twelve-month duration for active duty alerts. Like the FTC, we believe that twelve months is an appropriate period of time for consumers who request an active duty alert. For those who would like the alert to remain for more than twelve months, they have the ability to request a subsequent alert at the appropriate time. For others, the twelve months will be too long. Therefore, the statutory requirement of twelve months appears to be most appropriate.

Definition of "Appropriate Proof of Identity"

The FACT Act requires the FTC to determine what constitutes "appropriate proof of identity" as that phrase is used in Sections 605A, 605B, and 609(a)(1).[3] The FTC states that the standards of proof may need to vary depending on the circumstances, and that consumer reporting agencies are in the best position to assess the risks. TransUnion agrees and commends the FTC for developing a flexible approach in the Proposed Rule.

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 the relevant sections of the FCRA. Consumer reporting agencies must "ensure that the information is sufficient to enable the consumer reporting agency to match consumers with their files" and "adjust the information to be commensurate with an identifiable risk of harm arising from misidentifying the consumer." We appreciate the flexibility the FTC has provided, and we urge that it be retained in the Final Rule. We also ask the FTC to clarify that the information need only be of the type to allow the consumer reporting agency to match consumers with their files, not that consumer reporting agencies must ensure a match. We do not believe the FTC intended to impose an impossible standard of 100% match every time, and we hope to have this point clarified.

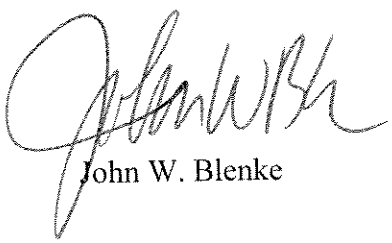
[3] Therefore, the Final Rule's definition of "appropriate proof of identity" would be limited to the listed sections and would not apply to other sections of the FCRA pertaining to identification of the consumer. We urge the FTC to acknowledge our understanding of the definition's applicability in the Supplementary Information of the Final Rule.

With respect to the examples provided by the FTC of information that might constitute reasonable information, we understand that the examples are illustrative only. However, we ask that a consumer's previous address (if the consumer has resided at the present address for less than two years) be an example of appropriate information. We also request that examples of additional proof of identity include copies of pay stubs and W-2 forms.

* * * * *

Once again, TransUnion appreciates the opportunity to comment on the Proposed Rule. If you have any questions regarding our comments, or if we may be of further assistance in connection with this matter, please do not hesitate to contact me at the number indicated above.

Respectfully submitted,



John W. Blenke