CDIA

CONSUMER DATA INDUSTRY ASSOCIATION

Empowering Economic Opportunity

June 15, 2004

Donald S. Clark
Secretary
Federal Trade Commission
Office of the Secretary
Room H-159 (Annex J)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20850

Re: FACTA Identity Theft Rule, Matter No. R411011

Dear Mr. Clark:

The Consumer Data Industry Association ("CDIA") respectfully comments on the Federal Trade Commission's ("Commission") proposed Identity Theft Rule. This rule would define certain new key terms in the Fair Credit Reporting Act ("FCRA"), as amended by the Fair and Accurate Credit Transactions Act ("FACT Act"). These terms are "identity theft," "identity theft report;" and "appropriate proof of identity." The rule would also determine the duration of an "active duty alert."

CDIA is an international trade association representing the consumer reporting industry. CDIA's members include the nationwide consumer reporting agencies as defined in section 603(p) of the Fair Credit Reporting Act ("FCRA").[1] As amended by the FACT Act, the FCRA imposes significant obligations upon consumer reporting agencies, particularly the nationwide consumer reporting agencies, with respect to consumers who may be victims of identity theft. These obligations are triggered when a consumer who is concerned about "identity theft" provides "appropriate proof of identity" and produces an "identity theft report." In addition, the FCRA, as also amended by the FACT Act, requires consumer reporting agencies to place an "active duty alert" in the file upon the request of a member of the armed services who qualifies for such an alert. Therefore, the terms that define the circumstances giving rise to these obligations will have a considerable impact on consumer reporting agencies.

[1] These agencies are identified as Equifax Information Services, LLC, Experian Information Solutions, Inc. and Trans Union, LLC.

Summary

CDIA concurs in the Commission's observations as to the importance of these definitions in protecting bona fide victims of actual or potential identity theft and the need to assure that the definitions will not enable the misuse of these protections to undermine the accuracy and integrity of consumer report information. In most respects the proposed rule's definitions appropriately balance the protection of victims with the need to prevent abuse of the system. CDIA believes, however, that in some important respects, the proposed rule and its illustrative examples create unnecessary ambiguity as to the definition of an identity theft report. This definition must include all the statutory elements of the definition of an identity theft, and it must allow consumer reporting agencies and information furnishers to rely upon authentic law enforcement reports and to validate these reports.

Comments

Identity theft significantly harms consumers, creditors and the integrity of consumer report information. CDIA and its members have implemented measures to address this crime and to help victims restore accurate credit information. CDIA worked with the FTC to develop the current voluntary fraud alert initiative, including automatic referral of fraud alert requests to other nationwide consumer reporting agencies. CDIA members regularly assist consumers who believe that information in their files is the result of identity theft. Through the E-OSCAR dispute resolution system, the nationwide consumer reporting agencies help consumers quickly remove or correct fraudulent trade-line information in their files.

In many respects, the FACT Act identity theft provisions reflect current industry practices to address identity theft, as well as those suggested by the FTC at its website: www.ftc.gov/idtheft. The FTC advises victims of identity theft to do the following:

1. Contact the fraud departments of any one of the nationwide consumer reporting agencies to place a fraud alert in the consumer's credit file (which will result in a referral of the fraud alert to the other two nationwide consumer reporting agencies).

2. Close credit accounts that the consumer knows or believes have been tampered with or opened fraudulently. Use the FTC's Identity Theft Affidavit when disputing new unauthorized accounts.

3. File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.

4. File a complaint with the FTC, which maintains a database of identity theft cases used by law enforcement agencies for investigations.

CDIA believes that the FACT Act identity theft requirements are intended to compliment existing industry and government measures designed to help identity theft victims. As the Commission observed, the statutory and regulatory definitions of "identity theft" and "identity theft report" are key to the implementation of the legal protections for these victims. The final rule's definitions must cover the circumstances that protect bona fide victims. At the same time, experience shows that some unscrupulous consumers will make false allegations to consumer reporting agencies in an attempt to remove accurate information from their files or to interfere with the rights of true victims of identity theft. The definitions must be broad enough to provide convenient relief to the victims, while not facilitating fraud or perpetuating identity theft.

A consumer's good faith suspicion that he or she has been or is about to become a victim of fraud or related crime, including identity theft, entitles the consumer to an initial fraud alert on his or her file at each of the nationwide consumer reporting agencies, as well as free access to the consumer's file at each of the nationwide agencies.[2] Upon presenting an identity theft report and providing reasonable cause to believe that an identity theft has occurred, the consumer may request an extended alert in his or her file at a nationwide consumer reporting agency, and may obtain two free credit reports within a twelve-month period.[3] In addition, the consumer's name will be omitted from any prescreened lists by the consumer reporting agency for five years.[4] Finally, with an identity theft report evidencing the consumer's identity theft claim, a consumer may identify information in his or her file that is the result of identity theft and may direct that the information be removed.[5]

The consumer's rights to fraud alerts and extended alerts apply only to the nationwide consumer reporting agencies. In addition to placing the appropriate alert in the consumer's file, a nationwide consumer reporting agency must refer the alert to the other nationwide agencies, and the consumer is entitled to free file disclosures at those agencies as well. The consumer's right to direct that the reporting of specified file information be "blocked" applies to all consumer reporting agencies, but only the nationwide consumer reporting agencies must refer the block request to the other nationwide agencies.

Although fraud alerts, extended alerts and file information blocks are each designed to help identity theft victims, each has different consequences with respect to the consumer's file at the consumer reporting agency. In the case of fraud alerts and extended alerts, the principal effect is to require creditors to undertake additional measures to verify the identity of the person requesting credit in the consumer's name.[6]

---

[2] FCRA § 605A; 15 U.S.C. § 1681c-1.

[3] FCRA § 605A(b)(1); 15 U.S.C. § 1681c-1(b)(1).

[4] FCRA § 605A(b)(1)(B); 15 U.S.C. § 1681c-1(b)(1)(B).

[5] FCRA § 605B(a); 15 U.S.C. § 1681c-2(a).

[6] Creditors may not open new credit accounts, issue new credit cards for an existing account or increase a credit limit unless the creditor uses "reasonable procedures to form a reasonable belief that the user knows the identity of the person" requesting the credit, new card, etc. In addition, the creditor must call a telephone number if it is provided by the consumer or take "reasonable

While this effect creates some difficulty for creditors, it may also interfere with consumers' ability to obtain credit and may significantly inconvenience the consumer. Because of the potential disadvantages to consumers from these file alerts, the additional benefit of free reports that accompany them may not provide sufficient incentive for unscrupulous consumers to falsely allege that they may be identity theft victims, or in the case of extended alerts, to provide a falsified identity theft report.

The same is not true in the case of an information block under section 605B. CDIA's members' experience with consumer report file information disputes shows that dishonest consumers will falsely claim that they have been identity theft victims and will provide falsified documents in support of those claims in order to have accurate, negative information removed from their files.

The FTC's supplementary information accompanying the proposed rule recognizes that the purpose for which the consumer provides the identity theft report (i.e., extended alerts or file information blocks) may determine how much information and detail a consumer reporting agency or a creditor may require when accepting an identity theft report. Because of the significant difference in the effect of an extended alert versus a file information block, CDIA fully supports this distinction and urges that it be reflected in the final rule.

CDIA offers the following specific comments on the proposed rule.

1. Definition of Identity Theft -- Proposed Rule § 603.2(a)

The proposed rule defines "identity theft" as "a fraud committed or attempted using the identifying information of another person without lawful authority." CDIA agrees with the Commission that, in order to trigger the important FCRA rights of potential identity theft victims and to enable them to avoid being actual identity theft victims, the definition should cover an attempted fraud, as well as the actual offense. CDIA notes, however, that an essential element of the offense is fraud or attempted fraud. The mere loss or theft of consumer's identifying information does not constitute identity theft. It may engender a good faith suspicion that the consumer could become a victim of identity theft and thus entitle a consumer to an initial fraud alert, but it does not provide the basis for an identity theft report.

The proposed definition of "identifying information" means "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," "including any telecommunication identifying information or access device as defined in 18 U.S.C. 1029(e)." The cited United States Code provision defines "access device" to include credit card and account numbers, mobile identification numbers, and personal identification numbers, that can be used alone or in conjunction

---

steps to verify the consumer's identity and to confirm" that the credit application is not the result of identity theft. In the case of an extended alert, the creditor *must* contact the consumer requesting the credit extension, etc. either in person, at the telephone number provided by the consumer or other reasonable contact method designated by the consumer.

with another access device to obtain money, goods, services or other thing of value. As a result of incorporating the US Code definition into the proposed rule, the rule's definition of identity theft could include the authorized use of a credit card, PIN or similar access device. CDIA understands that the Commission intends this result. However, affected industry members may not associate the crime of *identity* theft with the fraudulent use of a credit card number without identifying information. For that reason, in order to facilitate compliance, CDIA suggests that the final rule's definition of identifying information incorporate the current US Code definition of "any telecommunication identifying information or access device" The final rule could also provide that the definition would include the US Code definition as it may be amended, to reflect changes in technology. The portion of the definition of identifying information in Section 603.2(b)(4) of the final rule could read: "Credit card and other account numbers, mobile identification numbers and personal identification numbers, that can be used alone or in conjunction with another access device to obtain money, goods, services or other thing of value, and including any other telecommunication identifying information or access device as defined in 18 U.S.C. 1029(e)." Alternatively, the final rule could give current examples of what are included in "telecommunication identifying information or access device as defined in 18 U.S.C. 1029(e)."

CDIA agrees that an important element of the definition of identity theft is that the person's identifying information is used without lawful authority. As the Commission observes, individuals, such as guardians and attorneys-in-fact, may have lawful authority to use another's identifying information and may misuse that information to commit fraud. CDIA's members have experienced situations where consumers appear to have colluded with family members or friends to perpetrate a fraud or attempted fraud using their own identifying information. In those instances, the consumer refuses to prosecute the perpetrator of the fraud or attempted fraud. For that reason, CDIA believes that the final rule should provide that a consumer's refusal to prosecute the perpetrator of an identity theft is prima facie evidence that the consumer's identifying information was used with the consumer's lawful authority and thus does not involve identity theft.

2. Definition of Identity Theft Report -- Proposed Rule § 603.3(a)

The proposed rule defines "identity theft report" as a report (1) that alleges identity theft with as much specificity as the consumer can provide; (2) that is a copy of an official, valid report filed by the consumer with a Federal, State, or local law enforcement agency, including the United States Postal Inspection Service, the filing of which subjects the person filing the report to criminal penalties relating to the filing of false information, if, in fact, the information in the report is false; and (3) that may include additional information or documentation that an information furnisher or consumer reporting agency reasonably requests for the purpose of determining the validity of the alleged identity theft."[7]

[7] 69 Fed. Reg. 23377.

Although CDIA generally supports this definition, CDIA believes that additional clarification is necessary and strongly disagrees with the definition to the extent that it is predicated on the interpretation that an "official, valid" law enforcement report includes a complaint filed with the Commission's Identity Theft Clearinghouse.

a. Specificity Requirement and Examples of Specificity

The proposed definition requires that the report allege identity theft with as much specificity as the consumer can provide. CDIA supports this element of the definition, and suggests that the final rule and its examples make clear that the report must specify all the elements of the offense of identity theft.

The first example provides for "[s]pecific dates relating to the identity theft such as when the loss or theft of personal information occurred ***or*** when the fraud(s) using the personal information occurred, and how the consumer discovered or otherwise learned of the theft." 69 Fed. Reg. 23378 (emphasis added.). This example could be interpreted to mean that the loss or theft of personal information constitutes identity theft; however, the definition requires that the personal identifying information be used without lawful authority to commit a fraud or an attempted fraud. For that reason, we suggest that the definition of identity theft report require the consumer to provide as much specificity as possible as to each element of the offense: (i) the commission of a fraud or an attempted fraud, (ii) using the identifying information of another person, (iii) in an unlawful manner.

b. Requirement for an Official, Valid Law Enforcement Report

The Commission's Supplementary Information states that, under the FACT Act definition of identity theft report, which the proposed rule would expand upon, "a consumer could opt to use a copy of a complaint filed with the Commission's Clearinghouse as an "identity theft report" because such a copy would technically meet the statutory definition: it alleges identity theft, is filed with a federal law enforcement agency (i.e., the Commission), and, like all documents filed with federal agencies, is subject to criminal penalties for false filing (see 18 U.S.C. 1001)."[8]

CDIA respectfully disagrees with this observation. As the Commission also notes, its 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. Victims who have filed complaints with the Clearinghouse have done so voluntarily, with no guarantee of obtaining any immediate, direct benefit such as the investigation of their cases."[9] There is nothing about the FTC's Identity Theft Clearinghouse that would elevate a complaint filed electronically to the status of an "official" report. While FTC staff may consider the information for the purposes of evaluating identity theft trends and may, under certain circumstances, refer the information to law enforcement officials, there appear to be no established procedures for

[8] 69 Fed. Reg. 23372, n. 9.
[9] Id.

any FTC official to authenticate the information submitted in such a complaint. In fact, the consumer is given complete discretion in terms of how much information, including identifying information, the consumer wishes to provide. Nothing on the FTC's website alerts the consumer to the FTC's interpretation the complaint would subject the submitter to criminal penalties for filing false information. Indeed, because the consumer need not provide complete identifying information, such a representation would be an empty threat if it were made at all.

Moreover, the FTC's interpretation ignores the legislative history that Congress clearly intended the "valid, official" report to be a police report or similar law enforcement report. CDIA appreciates that only a minority of consumers who have self-identified themselves as victims of identity theft bothered to report the crime to the police. CDIA also recognizes that some consumers report difficulty in having the police accept a report of an identity theft crime.[10] For that reason, the statute defines an "identity theft report" to include a copy of "an official, valid report" filed with "a Federal, State or local law enforcement agency, including the United States Postal Inspection Service, or such other government agency deemed appropriate by the Commission," and the filing of which subjects the person filing the report to criminal penalties for false information in the report.[11] The fact that the identity theft report may be filed with law enforcement agencies other than a local police department does not alter the statutory requirement that the report be "valid" and "official."

The FTC's interpretation that the a consumer's complaint filed with the Commission's Clearinghouse would technically meet the statutory definition of an "identity theft report" is also at odds with the instructions to consumers at the FTC's website. As noted above, there the Commission recommends that consumers file *both* a police report *and* a complaint with the Commission's Clearinghouse. CDIA agrees that consumers should file both a police report (or comparable law enforcement report) and a complaint with the Commission, and CDIA agrees that the Commission's website appropriately distinguishes between the two submissions.

CDIA understands that the FTC's observation about a complaint submitted to its Identity Theft Clearinghouse was intended as a basis for providing that data furnishers and consumer reporting agencies may request additional information for the purpose of verifying the identity theft report. Nonetheless, under the FTC's interpretation, if a data furnisher or a consumer reporting agency receives a copy of a complaint that purports to be one submitted on its Identity Theft Clearinghouse, the rule would require that the additional information or documentation be "reasonably" requested for the purpose of determining the validity of the alleged identity theft. CDIA submits that, if the only "report" that the consumer presents is a copy of an on-line complaint submitted to the

---

[10] It is possible that some consumers who experience difficulty in this regard have experienced the loss or theft of identifying information, such as a wallet. While these circumstances may give rise to a good faith belief that the consumer could be a victim of identity theft and thus support a fraud alert, they do not constitute the elements of identity theft because no fraud or similar criminal offense has occurred. In that case, the police may not accept an identity theft report.

[11] FACT Act § 111; codified at FCRA § 603(q)(4); 15 U.S.C. § 1681a(q)(4).

FTC's Identity Theft Clearinghouse, it would always be reasonable for the data furnisher or the consumer reporting agency to request additional information or documentation. In fact, the FTC's website currently directs consumers to prepare a fraud affidavit to be submitted to consumer reporting agencies and data furnishers, in addition to filing a police report and a complaint with the Commission's Clearinghouse.

The final rule should make clear that a complaint filed with the FTC's Identity Theft Clearinghouse website is not a "identity theft report," and the rule should give examples of what constitutes a "an official, valid report" filed with "a Federal, State or local law enforcement agency, including the United States Postal Inspection Service, or such other government agency. The final rule should also make clear that if a consumer fails to provide an official law enforcement report, the consumer reporting agency shall have no further obligation predicated upon an identity theft report until the consumer provides such a report. Thus, if the consumer does not proffer an official law enforcement report, there is no obligation to determine the validity of the report or the veracity of the statements it contains.

c. Verification of Identity Theft Report

The proposed definition of an identity theft report includes "additional information or documentation that an information furnisher or consumer reporting agency reasonably requests for the purpose of determining the validity of the alleged identity theft." CDIA supports this verification element, which is consistent with the legislative history of the definition, and is essential to assuring that consumer reporting agencies and data furnishers will be able to take reasonable steps to authenticate the allegations and to protect themselves and the integrity of consumer report information. The verification element is also consistent with the FTC's identity theft website, which indicates that data furnishers and consumer reporting agencies will always be able to require a fraud affidavit in form and content similar to that found on the Commission's website.

In addition, the verification element is consistent with the FACT Act provisions, codified in FCRA section 609(e), with respect to the obligations of a business entity to disclose information to an identity theft victim. Those provisions give the entity the discretion *always* to request the following from the victim, in order to verify the ***claim*** of identity theft:

> (i) a copy of a police report evidencing the claim; ***and***
> (ii) a properly completed—
> (I) copy of a standardized affidavit of identity theft developed and made available by the Commission; or
> (II) an affidavit of fact that is acceptable to the business entity for that purpose.[12]

[12] FCRA § 609(e)(2)(B); 15 U.S.C. § 1681g(e)(2)(B)(emphasis added).

However, as discussed below, CDIA is concerned that the illustrative examples in the Proposed Rule appear to suggest that in some instances, it would be unreasonable for a consumer reporting agency to request a fraud affidavit or similar information when the consumer provides a police report. Such a suggestion would create unjustified inconsistency, because the FCRA itself permits furnishers to use their discretion to request such information in similar circumstances.

The proposed rule would require that any request for verification information or documentation be made not later than five business days after the date of receipt of the identity theft report or the consumer's request based upon the report, whichever is later. The Supplementary Information explains that a consumer reporting agency could accept an identity theft report for purposes of an extended alert, but could want additional information or documentation if the consumer later requests that certain information not be reported.[13] CDIA supports this provision, which it believes is consistent with the other provisions permitting increased scrutiny for information block requests.

The proposed time period for verification raises questions as to its relationship to the statutory time periods within which consumer reporting agencies and data furnishers must act upon consumer's requests that are based upon the identity theft report. A nationwide consumer reporting agency must institute an extended alert "beginning on the date of the request," and a consumer reporting agency must place an information block within four days of receipt of the consumer's identity theft report, along with the other statutory prerequisites.[14] Because both an extended alert and an information block request are triggered by the receipt of an identity theft report, the rule appears to provide that there is no obligation on a consumer reporting agency to act upon a consumer's request until the agency is able to authenticate the report. CDIA supports this provision and urges that the final rule make clear this result.

CDIA also suggests that the final rule provide for ten business days within which to request additional verification. Consumer reporting agencies will need a reasonable opportunity to review an identity theft report and determine whether verifying information is needed. Five business days may not allow for a meaningful review and determination.

d. Illustrative Examples -- Proposed Rule 603.3(c)

The proposed rule contains a number of examples with respect to what may be reasonable or unreasonable requests for additional information or documentation. Although these examples are for illustrative purposes only, CDIA believes that some clarification may be appropriate.

There are five examples of when it would or would not be reasonable to request additional information or documentation in addition to the official, valid report filed with a Federal, State or local law enforcement agency, the filing of which may result in

[13] 69 Fed. Reg. at 23372, n.11.

[14] *See* Sections 605A(b)(1)(a) and 605B(a); 15 U.S.C. §§ 1681c(b)(1)(a) and 1681c(B)(a).

criminal penalties if false. These examples are also illustrative. CDIA appreciates the attempt to balance the recipient's reasonable need for additional information with the convenience of the alleged victim. However, without additional clarification, the examples could imply that under some circumstances, requests for additional information or documentation are unreasonable, when that is not the case.

CDIA suggests the following clarifications to the proposed examples:

(1) **A law enforcement report containing detailed information about the identity theft and the signature, badge number or other identification information of the individual law enforcement official taking the report should be sufficient on its face to support a victim's request. In this case, without an identifiable concern, such as an indication that the report was obtained fraudulently, it would not be reasonable for an information furnisher or consumer reporting agency to request additional information or documentation.**

Although the example would permit requests for additional information if there is some indication that the report was obtained fraudulently, the example should also permit additional information if the report was fraudulently created or altered. Moreover, if the report is the basis for a request to block information in the consumer's file, it would be reasonable for the data furnisher or the consumer reporting agency to request more information connecting the identity theft to a fraud committed with respect to the information that is the subject of the fraud request.

For these reasons, CDIA suggests that the example should read:

A law enforcement report containing detailed information about the identity theft and the signature, badge number or other identification information of the individual law enforcement official taking the report should be sufficient on its face to support a victim's request. In this case, without an identifiable concern, such as an indication that the report was ~~obtained~~ fraudulently obtained, created or altered, it would not be reasonable for an information furnisher or consumer reporting agency to request additional information or documentation if the report is the basis for a request for an extended alert. If, however, the report is provided in connection with a request for a tradeline block or a cessation of information furnishing, it would be reasonable to request additional information connecting the identity theft to the information that is the subject of the request.

(2) A consumer might provide a law enforcement report similar to the report in paragraph (c)(1), but certain important information such as the consumer's date of birth or Social Security number may be missing because the consumer chose not to provide it. The information furnisher or consumer reporting agency could accept this report, but it would be reasonable to require that the consumer provide the missing information.

CDIA has no suggestions with respect to this illustrative example.

(3) A consumer might provide a law enforcement report generated by an automated system with a simple allegation that an identity theft occurred to support a request for a tradeline block or cessation of information furnishing. In such a case, it would be reasonable for an information furnisher or consumer reporting agency to ask that the consumer fill out and have notarized the Commission's Identity Theft Affidavit or a similar form and provide some form of identification documentation.

CDIA interprets the import of this illustrative example to be that it is reasonable for an information furnisher or a consumer reporting agency to request a notarized copy of the Commission's identity theft affidavit when a consumer has not filed a report with a law enforcement official that may review the report. CDIA supports this example. However, as indicated above, CDIA respectfully disagrees that a complaint filed on the FTC's Identity Theft Clearinghouse website would constitute an "official" law enforcement report. CDIA also suggests that the illustrative example indicate that the "similar form" to the Commission's Identity Theft Affidavit be one that ties the alleged identity theft to the information that is the subject of the block request.

Moreover, the example should make clear that a purported law enforcement report generated by an automated system must include some acknowledgement or other independent record that it was, in fact, submitted to the law enforcement agency. The final rule should also provide that a copy of a "screen shot" of an alleged report will not constitute a valid, official law enforcement report, and may be rejected by a consumer reporting agency or information furnisher without reviewing any other documentation.

(4) A consumer might provide a law enforcement report generated by an automated system with a simple allegation that an identity theft occurred to support a request for an extended fraud alert. In this case, it would not be reasonable for a consumer reporting agency to require additional documentation or information, such as a notarized affidavit.

The distinction between this example and the preceding one appear to illustrate that consumer reporting agencies may need more information to authenticate a identity theft report submitted by a consumer when the purpose is an information block request than when the request is for an extended alert. As discussed above, CDIA supports this distinction. However, to the extent that the Commission assumes that a simple allegation submitted on the FTC's Identity Theft Clearinghouse would constitute a "law enforcement report generated by an automated system with a simple allegation that an identity theft occurred," CDIA believes that such an interpretation is unsupported by the FACT Act and its legislative history.

(5) If the information the information furnishers or the consumer reporting agencies are seeking is already found in the law enforcement report which is otherwise satisfactory, it would not be reasonable to request that the consumer fill out the same information on a different form.

The point of this example is unclear. The example may intend to illustrate that all the information needed to authenticate an identity theft report is included on the form, it would not be reasonable to require the completion of another form for the purpose of having the information be contained on that form. However, if the form submitted by the consumer is a "law enforcement report generated by an automated system with a simple allegation that an identity theft occurred," such a form may not have been submitted to a law enforcement official, the form may not have indicated that the false filing would submit the filer to criminal penalties, etc. In other words, there may be many reasons why an information furnisher or a consumer reporting agency would want to require a notarized form or other means of authenticating the consumer's representations. This example should be clarified to permit a consumer reporting agency or information furnisher to seek additional information in the form of an affidavit, such as the FTC form of affidavit or similar form. As discussed above, the FTC's identity theft website currently anticipates this procedure, and it should be permitted in the final rule.

3. Duration of an Active Duty Alert -- Proposed Rule 613.1

The FACT Act amended the FCRA to protect active duty members of the armed forces and reservists called to duty when they are assigned to service away from their regular duty station, such as in Iraq. These service men and women or their personal representatives may place "active duty alerts" on their files at nationwide consumer reporting agencies to alert creditors and others of their situation. The Act provides that such an alert shall be in effect for 12 months, unless the Commission by regulation provides for a longer period.

The Commission proposes to limit the duration of the active duty alerts to 12 months. CDIA supports this time period. The active duty alerts are intended to protect servicemen and women during the time that they are temporarily away from their regular duty station. As the Commission observed in its Supplementary Information, these temporary assignments generally last for less than 12 months. If a member of the armed services is then reassigned to a new duty station, the need for the alert would no longer apply. At the same time, if an armed services member is posted away from the regular duty station for a period longer than 12 months, he or she could renew the alert at the end of the 12-month period. For these reasons, the statutory time period of 12 months is adequate and reasonable, and should be adopted in the final rule.

4. Appropriate Proof of Identity -- Proposed Rule 614.1

In order to receive the protections of a fraud alert, an extended alert or a file information block, a consumer must provide "appropriate proof of identity," in addition to the other statutory requirements. In the Supplementary Information, the Commission recognizes the significant risk of harm to consumers if an imposter is able to obtain access to a consumer's file in order to remove a fraud alert or an extended alert. The Commission also recognizes that the consumer reporting agencies need to have flexibility in matching the consumer's proof of identity to information in their files.

Accordingly, the proposed rule would require consumer reporting agencies to develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity for purposes of FCRA sections 605A, 605B, and 609(a)(1). In developing these requirements, the consumer reporting agencies must (i) ensure that the information is sufficient to enable the consumer reporting agency to match consumers with their files and (ii) adjust the information to be commensurate with an identifiable risk of harm arising from misidentifying the consumer.

CDIA believes that the final rule should assure that consumer reporting agencies retain flexibility to determine how much identifying information they need in order to be confident of an accurate verification of the consumer's identity.

CDIA suggests two modifications to the illustrative examples. First, in the example of identification information for a consumer file match in proposed section 614.1(b)(1), the information should include the consumer's previous address if the consumer has resided at the present address for less than two years.

In the second example, relating to additional proof of identity, there is a reference to "current" methods of authentication. It is unclear what is meant by "current" methods. CDIA also suggests that the final rule include as examples of alternative proof of identity copies of pay stubs and W-2 forms.

CDIA notes that the proposed rule's definition of appropriate proof of identity applies only to the requirements of FCRA sections 605A, 605B, and 609(a)(1)(A). The Act's requirements for proper identification for file disclosures under the other provisions of section 609 are found in section 610(a)(1) and are unaffected by the proposed rule's definitions. CDIA suggests that the Commission's Supplementary Information to the final rule include this observation.

CDIA appreciates the opportunity to comment on this important rule.

Sincerely yours,

Stuart K. Pratt
President