Consumers Union
Publisher of Consumer Reports

West Coast Office
1535 Mission St.
San Francisco, CA 94103
415-431-6747 (phone) 415-431-0906

June 8, 2004

Federal Trade Commission
Office of the Secretary
www.regulations.gov

Re: FACTA Identity Theft Rule, Matter No. R411011

Comments of: Consumers Union, Consumer Action, Consumer Federation of America, Electronic Privacy Information Center, Identity Theft Resource Center, National Consumer Law Center, National Association of Consumer Advocates, National Council of La Raza, Privacy Rights Clearinghouse, Privacy Times, and U.S. PIRG.

Summary of comments

We offer these comments on the proposed rule on identity theft definitions, the duration of active duty military alerts, and the appropriate proof of identity under the Fair Credit Reporting Act.

Our primary concern is that the definition of identity theft report is too open-ended. The definition will introduce many problems by permitting each CRA and furnisher to require different additional information before a sworn statement filed with a law enforcement agency qualifies as an identity theft report. The first problem is that consumers will never know at the time they file a request for a fraud alert or a block if their document meets the definition of an identity theft report. Second, consumers will have to assemble different packets of information to meet the varying requirements of different CRAs and furnishers, a result contrary to the goal of FACTA to make it easier for identity theft victims to eliminate the consequences of ID theft. Third, the delay inherent in a request and reply process before the report can meet the definition of an ID theft report will degrade the value of the extended fraud alert. The value and certainty of using an extended fraud alert to stop an ongoing series of thefts in its tracks will be lost if the initial submission of a report filed under penalty of perjury with a law enforcement entity does not, by itself, constitute an ID theft report and thus immediately trigger the right to an extended fraud alert.

For these reasons, we oppose adding any additional requirements for information before a statement filed with any law enforcement agency under penalty of

perjury can qualify as an identity theft report for purposes of triggering the right to an extended fraud alert.

We also respectfully suggest that the definition of an identity theft report is not the right place to address any furnisher or CRA need for additional information before processing a trade line blocking request. However, if the Commission pursues this approach, it must at least provide one document that an ID theft victim can file with all CRAs for an extended fraud alert and with all CRAs and furnishers to invoke trade line blocking. Any document containing that information solicited by the FTC ID Theft Affidavit which is reasonably available to the consumer should qualify to trigger these rights.

In addition to our fundamental concern about the definition of an ID theft report, we also suggest that the military alert period is too short, that any requirement of absence of lawful authority be restricted to express, actual and lawful authority; that the rule expressly prohibit excessive identification requirements; that the rule include reporting requirements; and that the rule require CRAs to make fraud alerts and trade line blocking available to persons who request these services in Spanish.

Questions Posed by the Commission

A. Questions relating to the definition of identity theft

A.1. Does the term "identity theft" as defined by the Act need further definition?

No. The statutory definition is broad, flexible and illustrative, rather than exhaustive. This is important because identity theft practices are fast-changing. A regulatory definition which excludes future kinds of identity theft could quickly become outdated, causing problems for consumers.

A.2. Should the Commission define the term "identifying information" to have the same meaning as "means of identification" in 18 U.S.C. § 1028(d)(4) [sic: (1028(a)(7)]?

Yes. We support this definition because of its inclusiveness. This definition should accommodate new kinds of identifiers used in the future.

A.3. Should the Commission add the element of "attempts" to the definition of the term "identity theft?"

Yes. An attempt to impersonate a consumer triggers the need for a consumer to take preventative steps, such as the placement of a fraud alert. Defining identity theft victims to include targets of uncompleted or unsuccessful attempts will allow consumers to act when they first learn of a thwarted attempt to use an element of

their identities. In addition, as the Commission's explanatory material points out, even unsuccessful attempts to impersonate a consumer may count as a credit file inquiry, affecting the consumer's credit score. An inquiry stemming from an unsuccessful theft attempt may also cause the consumer to be flagged by a creditor model which uses a statistical formula that includes inquiries to monitor existing credit accounts for closer scrutiny of payment patterns or credit limits.

A.4. Should the Commission add the element that a person's identifying information must be used without such person's knowledge to the definition of the term "identity theft"?

No. In many cases, the identity theft victim will not know that his or her information is being used by the thief. However, there may be situations involving family abuse where the victim has knowledge of but no power to stop the activity. Elder abuse and spousal abuse could fall into this category. A person who knows that a crime is being committed against himself or herself is no less a victim of that crime.

A.5. Should the Commission add the element that a person's identifying information must be used without such person's lawful authority to the definition of the term "identity theft"?

No. A key purpose of FACTA was to provide additional protection to identity theft victims. Imposing added preconditions not required by the statute is unlikely to be consistent with that purpose, particularly when there is no demonstrated need for those preconditions. The theft of the identities of children by their legal guardians could pose special issues if the definition includes a requirement of lack of legal authority. The explanatory language which suggests that a legal representative never has the power to defraud the other person is helpful, but adding this kind of requirement is likely to make it much harder for a newly adult person to remove from his or her credit record transactions not fairly attributed to that person, when those transactions were initiated by a legal guardian.

We are also concerned that "lawful" authority might be in interpreted differently than express, actual authority. Consumers should not have to face assertions that a thief who had no actual, express authority had ostensible authority, perhaps because the thief gained access to consumer's identifying information in a way that the consumer might have prevented by heightened home security. If an "authority" approach is used at all, it should be tied to the existence only of express actual authority. Thus, if the concept of "lawful authority" is used, it should at least be modified to require "<u>express, actual and</u> lawful authority."

A.6. Are there additional elements that the Commission should add to the definition of the term “identity theft”?

No. Added elements would reduce the inclusiveness, and hence the flexibility, of this important definition.

B. Questions relating to the definition of identity theft report

B.1. Does the term “identity theft report” as defined by the Act need further definition?

Yes, this definition must be fundamentally changed, as described below. First, a few technical suggestions. The word “reasonably” should be added to section 603.3(a)(1), before “provide,” and the phrase “to the extent requested on the report form and known to the consumer at the time the report is filed.” A report should not be deemed insufficient if it gives all of the information requested by the report form which was reasonably available to the consumer at the time the report was filed.

Similarly, section 603.3(b) should be expressly qualified by adding “to the extent known to the consumer at the time the report is filed” after “as follows.” Finally, section 603.3(b)(4) should refer to “Other reasonable” information rather than to “Any other information.”

The proposed regulation’s definition of an identity theft report is fundamentally flawed. The flaw comes from defining the report to include additional information requested by the CRA or furnisher. The proposed definition is a radical departure from the statutory concept that the consumer must simply file something with a law enforcement agency which is accompanied by criminal penalties for false filings. As currently drafted, the proposed definition provides no certainty to a consumer who has already filed a sworn statement with a law enforcement agency. The consumer simply can’t tell whether or not a report meets the definition of an identity theft report. Indeed, because the definition allows each CRA, and each furnisher, to impose different information requirements to satisfy the definition of an identity theft report, a document may constitute an identity theft report with one CRA and not with another, or with the CRAs but not with one or more information furnishers. A further flaw is that the consumer will not even know if what he or she has filed meets the definition of an identity theft report until five business days pass, and even longer if the CRA or furnisher seeks added information.

The definition should be revised to track the statutory requirement that an identity theft report is a statement alleging identity theft that is filed with a law enforcement agency subject to criminal penalties for false filing. This would require deleting section 603.3(a)(3). Any issues related to a need for more

information before processing a request for a trade line block should be separated from the definition of an identity theft report.

It boggles the mind to suggest that a consumer who has been impersonated at six creditors must file six different documents in order to have an identity theft report sufficient to support a request for trade line blocking for each of those furnishers. Even if reasonably available and reasonably necessary additional information may have to be provided in order to complete a request for a block, placing such requirements in the definition of an identity theft report will create insoluble problems. Here are just some of the problems with the approach taken in proposed definition.

First, the proposed definition will create a bewildering situation in which one consumer could be required to augment a single police report in different ways for different CRAs and different furnishers in order to meet the basic definition of an identity theft report. It will be impossible for the Commission, consumer groups, or even CRAs and creditors to tell consumers what to file to constitute an identity theft report.

Second, the definition can never be initially satisfied if either the furnisher or the CRA asks for more information within five business days. This means that consumers will not know for at least five business days whether or not the consumer has met the statutory requirements, and the time delay could be even longer if the CRA or furnisher seeks more information.

Third, a definition that allows the CRA or furnisher discretion to decide what and how much additional information to require before the definition can be satisfied will open the door to abuse by furnishers or CRAs who wish to make it difficult to exercise the right to trade line blocking.

Fourth, there is a special problem with defining the triggering document for placement of an extended alert—the identity theft report—so that there is a built in delay before the requirement is triggered. If the definition continues to give the CRA five business days to seek more information, a consumer could never be certain until after that time has passed that an ID theft report has been filed, triggering an extended alert. Although; in theory, a consumer could first place an initial alert and then seek an extended alert—this would require increased consumer sophistication. It would also force consumers who have already become victims to take two steps—placing an initial plus an extended fraud alert just to be sure that there is no delay caused by an additional information request before the extended alert begins. This would be an added burden on both consumers and CRAs.

The identity theft definition is simply not the place to address concerns related to the possibility of abuse of the right to block identity theft generated information. Instead, the statute already permits the information furnisher or the CRA to reject

or reverse a block in certain circumstances. Any additional requirements for information and documentation and any consequences for failing to provide that additionally required information should be addressed in connection with rejecting or reversing a requested block, and not in the definition of an identity theft report.

Examples (c)(2) and (c)(3) further illustrate the problem of tying the definition of an identity theft report to a response to the request for additional information. Example (c)(2) suggests that a furnisher or a consumer reporting agency could accept a report which does not include a consumer's date of birth or Social Security Number, but the CRA also could choose to insist upon these identifiers—even when they are not necessary to match the consumer to the file. If the law enforcement agency did not require this information from the consumer in order to file a report under penalty of perjury, the CRA should not be able to require that same information as a precondition to the existence of an identity theft report. If the CRA were to need additional information in order to adequately identify the consumer, that requirement is properly placed under the appropriate identification section, and not in the definition of the identity theft report.

Example (c)(3) is an even stronger illustration of the problems with insisting on additional indicia of seriousness in order to satisfy the definition of an identity theft report. This example suggests that each information furnisher and each CRA could decide whether the additional information to be required would be the ID theft affidavit or some other form, which might also have to be notarized. Will a consumer impersonated at six creditors have to pay six notary fees? This example permits that result by allowing each furnisher to insist on its own form. However, it makes no sense to say that the one document, filed under penalty of perjury with one enforcement agency, and giving all of the information requested by that law enforcement agency on its own form, is an identity theft report for some purposes and not for other purposes.

We strongly recommend that any perceived need for additional detail be separated from the definition of the identity theft report itself. The Commission has adequate authority to provide guidance with respect to what information can be required by an information furnisher or a CRA to reject or reverse a block; this issue simply should not be dealt with under the definition of an identity theft report.

If, however, the Commission pursues this deeply flawed approach, we respectfully suggest that two key changes be made. First, the simple report filed with law enforcement must always meet the definition of an ID theft report for purposes of triggering an extended fraud alert. Second, the regulations must designate a single document that will always be sufficient to constitute an identity theft report with any CRA or furnisher. A single, plainly identified document is essential to eliminate the delay, cost, inconvenience, and plain

incomprehensibility of the system contemplated by the proposed regulation, in which each CRA and each furnisher can insist on a response to a different information request before the consumer will have an ID theft report with respect to that CRA or furnisher. The proposed regulation should at least be revised to provide that a consumer who files both a report with a law enforcement agency and the information solicited by the FTC ID Theft Affidavit has always satisfied the ID theft report requirement.

B.2. Should the Commission define what is an "appropriate law enforcement agency?"

No. All law enforcement agencies should qualify. The helpful statement in the explanatory material that a complaint which is sent to the Commission's database is a report to a law enforcement agency should be included in the rule. Because of the difficulties consumers continue to face in filing police reports, it is very important that a report filed with an automated complaint system, including the Commission's system, qualify as an Identity Theft Report—as it clearly does under the statutory definition.

B.3. Will criminal penalties for false filing of an identity theft report deter abuse of the credit reporting system? Will those penalties be effective if they apply to a report filed by automated means?

Yes and yes. The vast majority of consumers will take seriously a statement made to law enforcement, and the report form often will say that the report is made under penalty of perjury. The few who may be out to falsely clean up a credit file, rather than to remove the consequences of an ID theft, may not be deterred by a face to face meeting at the local police department, since their intention is civil, not criminal. The Commission could address the issue of credit repair companies that advise the false filing of complaints by separately pursuing these companies as aiders and abettors of perjury.

B.4. Are the examples useful?

The examples should be revised because the definition itself must be revised. The proper balance has not been struck in the examples because of the inherent harm described in response to question B.1, from placing the permission to seek more information into the definition of an identity theft report. This puts the burden of delay on the consumer in a way that interferes with a remedy (the extended alert) which is designed to be promptly available in order to cut off an existing pattern of criminal activity. This issue is discussed above.

In addition, the rule and the examples give too much discretion to the credit reporting agencies and to information furnishers to insist on detailed information which may not be reasonably needed and may not be reasonably available to the victim. This approach tips the balance too far against legitimate use of the new rights conferred upon identity theft victims by FACTA.

Example (c)(2) also permits a requirement for a Social Security Number as a precondition to meeting the definition of an identity theft report. We are strongly opposed to the portion of the example which suggests that it is appropriate to require a consumer who has been a victim of identity theft to provide the full nine digits of the Social Security Number. Matching requirements for consumers to exercise their identity theft prevention rights under FACTA should be no more stringent than the level of matching which the CRAs require from users of credit files. Consumers are understandably reluctant to give their Social Security Numbers. Consumers who have been victims or who are concerned about becoming victims of identity theft may be even more concerned about safeguarding this number. If a CRA or furnisher is permitted to request a Social Security Number at all (to place an alert or a block), it should be limited to the last four digits of the Social Security Number, rather than the entire number. We agree, however, that more stringent matching should be required to remove alerts than to place them.

C. Questions relating to the duration of active-duty alerts

C.1. Should the Commission maintain the duration of the active-duty alert at the minimum statutorily determined length of 12 months as proposed?

No. Twelve months is too short a time given the uncertainties of wartime service, which may call for longer deployments. It is simply not reasonable to require a person who is already out of country serving our nation to take the additional step of extending a previous employee's military alert. Military personnel who are on short deployments and wish for a shorter military alert can simply remove the alert when they return to the U.S.

C.2. Should the Commission set an alternate length of time for the duration of an active duty alert?

Yes. An active duty military consumer should have at least the option of placing an open-ended alert which remains in place until the consumer takes an affirmative step to remove it. Another possibility is that the alert could be open-ended, but expire automatically three months after the expected release from service date, which could be requested when the alert is placed.

An alternative to an open-ended alert would be for the regulation to provide either a three-year effective period for the alert, or to provide a period of from 12 to 36

months, with the time set at 36 months unless the military consumer asks for a shorter time between 12 and 36 months.

The Commission should consider and resolve by regulation a related issue arising from the definition of active duty military consumer, which appears to require that the consumer be away from his or her usual duty station. The Commission should define "away from the usual duty station" to include a regular posting to a duty station outside of the 50 states. This definition would give equal protection to military personnel who are serving a multiple-year tour of duty at a base outside of the U.S. These military personnel could then make an individual choice about whether or not to use the available protection.

C.4. How difficult will it be for active duty military consumers to place or have a personal representative place another active duty alert if the initial alert expires before the end of the term of deployment?

It will be difficult for some. While many service members do have a personal representative, others, particularly those without spouses, may not wish to give another person access to their credit record.

D. Questions relating to appropriate proof of identity

D.1 Should the Commission set standards for what constitutes appropriate proof of identity?

Yes, but it also should expressly prohibit excessive identity requirements. Consumer advocates are concerned that CRAs and, in particular, furnishers may insist on heightened identification requirements in order to make it more difficult to access the rights conferred on identity theft victims by Congress.

To prevent this undesirable outcome, while still preserving flexibility, the rule itself should prohibit excessive identification standards. For placing an alert, and for trade line blocking, the rule should prohibit requiring more information than the level of information sufficient to enable the consumer reporting agency to match consumers with their files. The amount of identifying information must not be more than is reasonably necessary in light of the risk to the consumer of a delay in the exercise of an identity theft prevention right.

The reference in section 614.1(a)(ii) that requires that the information be commensurate with an identifiable risk of harm from misidentifying the consumer is useful. We suggest, however, that the rule be augmented by adding these requirements to 614.1(a):

(iii) that the information required not be more than is reasonably necessary to identify the consumer for the purpose of matching the consumer with his or her file;"

(iv) that the required identifying information be disclosed to consumers before the request;

(v) that in developing and implementing reasonable requirements for proof of identity, each CRA must ensure that the proof of identity requirements do not prevent prompt, same-day placement of an alert and do not restrict access to trade and blocking; and

(vi) that, for purposes of referral to place a fraud alert, each CRA must accept the identifying information obtained by the other CRA, and cannot impose additional CRA-specific requirements before honoring the alert request.

These modifications will help to prevent use of heightened identification requirements to block the exercise of consumer rights. There is no need for a high identification standard for placing fraud alerts and for blocking. Both already require an identity theft report, a document filed with a law enforcement agency or other agency recognized for this purpose by the Commission and exposing the filer to a risk of criminal penalties for false filing. There is far less risk that a thief or abuser would attempt to place an inappropriate fraud alert or trade line block than there is that a thief would try to get a consumer's credit report. It is highly unlikely that someone other than the consumer would attempt to block a trade line or to impose identification preconditions on future credit.

The approach of the rule of allowing each consumer reporting agency and furnisher to develop and implement reasonable identification requirements for sections 605A (for CRAs) and 605B (for CRAs and furnishers) is troublesome for another reason. This approach may defeat the FACTA goal of permitting consumers to request an alert from one of the three major credit reporting agencies, and have that alert forwarded to the additional agencies. If each agency has a different set of identification requirements, how will referral of fraud alert requests work? The statutory goal cannot be served if the request is made, but is not honored, because of differing identification requirements among CRAs. In that situation "one call" doesn't "do it all."

The rule should specifically address the risk to a consumer that it will be difficult to meet the proof of identity requirements in order to place an alert on a credit file which has already been partially corrupted by changes made by a thief. A consumer must be able to alert current and future creditors to the activities of an impostor through an extended fraud alert even if the impostor has already succeeded in changing the consumer's street address as shown in the credit file, or has succeeded in opening a credit file in a different name but using the consumer's Social Security Number. Thus, while we oppose allowing CRAs to

require a consumer to provide his or her full Social Security Number in order to identify her or himself for a fraud alert, if a consumer does provide a full Social Security Number, that consumer should be entitled to place a fraud alert on all credit files carrying that Social Security Number, even if one or more of those credit files shows a different name.

Finally, the rule also should require that the identification requirements must not prevent a consumer from placing an alert on the same day that the alert is requested. Thus, if a CRA's automated system cannot be satisfied, there should be a mechanism to fax in the required information. A CRA should not be permitted to require a Social Security Number or a copy of a passport to place an extended alert. Instead, a copy of a government-issued photo identification plus a bill in the consumer's name should be satisfactory. In a two-earner household, all the bills may be in the name of only one of the adults. If a utility or similar bill is required, it should be enough that the billing address matches the address on the government-issued identification card. The rule should clarify there must be a way to place an initial and an extended alert immediately even if the information in the credit file has been partially modified by a thief.

D.2. Are the examples useful?

Example one contains information which is too specific. We are deeply concerned that the level of detail given in these examples will encourage CRAs to seek too much identifying information, which will cause a delay in the placement of alerts. If the CRA is able to match the consumer to the file without the middle initial, for example, or in spite of the fact that the consumer has provided a full middle name rather than a middle initial, this should not prevent the consumer from promptly placing a fraud alert.

A consumer should not have to give the full nine digits of the Social Security Number in order to identify himself or herself to a CRA in order to place an alert, even if the consumer would have to provide that same level of identity to secure a copy of the report. There is very little risk that an identity thief will try to place a fraud alert. Similarly, a thief is highly unlikely to attempt to clean up someone else's credit file. For this reason, it is simply not necessary to require a high level of identification of the consumer before giving the consumer access to the statutorily mandated rights to fraud alert and blocking. The "additional proof" items in example two should be things that can substitute for the items in example one, not items that can be required in addition to the example one items. Example two should be characterized as "alternative proof of identity," not as "additional proof of identity."

D.3. Has the Commission adequately balanced the harm from delay and the risks of misidentification?

No. To do so, the rule should be augmented to describe situations where no information beyond the full name and current, or current plus prior, street address, and the date of birth may be required. This would involve adding to section 614.1 the language suggested in response to question D.1, plus examples of when additional information should not be required, just as similar examples are given in section 603.3(c).

The regulations should require reporting to ensure definitional and identification requirements are not abused by CRAs.

To ensure that CRAs do not use any discretion this rule may give them to deprive consumers of access to identify theft prevention and correction rights, the regulations should include reporting requirements for the CRAs. These requirements should include statistics about the number of requests for an extended fraud alert that each CRA rejects or delays on the grounds that more information is required, the nature of the additional information requested, and whether the information request results in a delay in, or in non-placement of, the extended alert. Similarly, for requests for trade line blocks, each CRA should be required to report the number of requests for trade line blocking which are declined or rescinded for: a) errors, b) material misrepresentations, c) where the consumer obtained goods/services, and d) where the report allegedly is not specific enough or where the CRA requests more information.

The regulations should mandate language access to fraud alerts and blocking

Multilingual access is crucial for placement of an initial or extended fraud alert, trade line blocking, and requesting a free report. Multilingual telephone access is particularly needed for alerts and blocking. Multilingual access should be required for at least the top five non-English languages spoken in the U.S. In other contexts, consumer and civil rights advocates often suggest that at least the ten largest language groups per geographic area should be served. A more detailed comment letter filed in matter under FACTA Free File Disclosures Rule, Matter R411005, addressed the need for Spanish language access to fraud alerts, blocking and free credit reports. We incorporate that comment letter, dated April 15, 2004, as part of these comments.

We look forward to FACTA regulations that will benefit consumers, deter thieves, and improve the accuracy and accessibility of data which is used for credit evaluation. The proposed regulations cannot do so without significant revisions.

Very truly yours,

Gail Hillebrand
Consumers Union of U.S., Inc.
West Coast Office
1535 Mission St.
San Francisco, CA 94103

Ken McEldowney
Consumer Action

Brad Scriber
Consumer Federation of America

Chris Hoofnagle
Electronic Privacy Information Center

Linda Foley
Identity Theft Resource Center

Anthony Rodriguez
National Consumer Law Center

Brenda Muñiz
National Council of La Raza

Ira Rheingold
National Association of Consumer Advocates

Beth Givens
Privacy Rights Clearinghouse

Evan Hendricks
Privacy Times

Ed Mierzwinski
U.S. PIRG

Suggested Changes to Proposed Regulations

Sec. 603.2 Identity theft.

(a) The term “identity theft” means a fraud committed or attempted using the identifying information of another person without express, actual, and lawful authority.

(b) The term “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--

(1) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(3) Unique electronic identification number, address, or routing code; or

(4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

Sec. 603.3 Identity theft report.

(a) The term “identity theft report” means a report--

(1) That alleges identity theft with as much specificity as the consumer can reasonably provide to the extent requested on the report and known to the consumer at the time the report is filed;

(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~~

Preferred Alternative: Delete (3)

~~(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, provided that the information furnisher or consumer reporting agency makes such request not later than five business days after the date of receipt of the copy of the report form identified in paragraph (a)(2) of this section or the request by the consumer for the particular service, whichever shall be the later.~~

Second Alternative: Revise (3)

(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, before responding to a request for trade line blocking or to cease information furnishing, provided that the information furnisher or consumer reporting agency makes such request not than five business days after the date of receipt of the copy of the report form identified in paragraph (a)(2) of this section or the request by the consumer for

the particular service, whichever shall be the later, and further provided that: i) an unnotarized copy of the ID Theft Affidavit is sufficient to satisfy any such request, and ii) that the request and all information offered about what constitutes an identity theft report for purposes of information cessation or trade line blocking clearly discloses that an unnotarized copy of the ID Theft Affidavit may be required in addition to or as part of a report.

(b) Examples of the specificity referenced in paragraph (a)(1) of this section are provided for illustrative purposes only, as follows, to the extent known to the consumer at the time the report is filed:

(1) Specific 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.

(2) Identification information or any other information about the perpetrator, if known.

(3) Name(s) of information furnisher(s), account numbers, or other relevant account information related to the identity theft.

(4) ~~Any other~~ Other reasonable information known to the consumer about the identity theft at the time the report was filed.

(c) Examples of when it would or would not be reasonable to request additional information or documentation referenced in paragraph (a)(3) of this section are provided for illustrative purposes only, as follows:

(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.

(2) A consumer might provide a law enforcement report similar to the report in paragraph (c)(1) of this section, 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, if necessary to identify the consumer under section 614.1.

(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 trade line 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 ID Theft Affidavit ~~or a similar form~~ and provide some form of identification 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.

(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.

Section 603.3A Reporting Required.

(a) Consumer reporting agencies shall file annually a full and complete report describing:
(1) The number of requests for extended fraud alerts granted based on the initial submission of a consumer,
(2) The number of requests for extended fraud alerts delayed due to a request by the CRA for additional information to satisfy the requirement for an ID theft report, and the nature of the additional information requested,
(3) The number of requests for extended fraud alerts that do not result in placement of an alert after more information is requested,
(4) The average delay between the request for an extended fraud alert and placement of the extended alert,
(5) The number of requests for trade line blocking granted based on the initial submission of the consumer,
(6) The number of requests for trade line blocking delayed due to a request by the CRA for additional information to satisfy the requirement for an ID theft report, and the nature of the information requested,
(7) The number of requests for trade line blocking that do not result in placement of a block after more information is requested,
(8) The average delay between the request for trade line blocking and placement of the block,
(9) The number of trade line block requests declined or rescinded because the agency reasonably determined that there is an error in the request,
(10) The number of trade line block requests declined or rescinded because the agency reasonably determined that there was a material misrepresentation of fact by the consumer, and
(11) The number of trade line block requests declined or rescinded because the agency reasonably determined that the consumer obtained possession of goods, services, or money as a result of the blocked transaction.
(b) Such reports shall be made available to the public on the Commission website

Sec. 613.1 Duration of active duty alerts.

The duration of an active duty alert shall be ~~12~~ 36 months.

Sec. 614.1 Appropriate proof of identity.

(a) Consumer reporting agencies shall 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 Fair Credit Reporting Act. 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;

(ii) adjust the information to be commensurate with an identifiable risk of harm arising from misidentifying the consumer;

(iii) that the information required not be more than is reasonably necessary to identify the consumer for the purpose of matching the consumer with his or her file;"

(iv) that the required identifying information be disclosed to consumers before the request;

(v) that in developing and implementing reasonable requirements for proof of identity, each CRA must ensure that the proof of identity requirements do not prevent prompt, same-day placement of an alert and do not restrict access to trade and blocking; and

(vi) that, for purposes of referral to place a fraud alert, each CRA must accept the identifying information obtained by the other CRA, and cannot impose additional CRA-specific requirements before honoring the alert request.

(1) Ensure that the information is sufficient to enable the consumer reporting agency to match consumers with their files; and

(2) adjust the information to be commensurate with an identifiable risk of harm arising from misidentifying the consumer.

(b) Examples of information that might constitute reasonable information requirements for proof of identity are provided for illustrative purposes only, as follows:

(1) Consumer file match: The identification information of the consumer including his or her full name (first, middle initial, last, suffix), any other or previously used names, full address (street number and name, apt. no., city, State, and ZIP Code), full 9 digits of Social Security number, and/or date of birth.

(2) ~~Additional~~ Alternative proof of identity: copies of government issued identification documents, utility bills, and/or other current methods of authentication of a person's identity which may include, but would not be limited

to, answering questions to which only the consumer might be expected to know the answer.

(3) For the purposes of placing an alert, a trade line block, or a request to cease furnishing information, the degree or level of information required may not exceed the degree or level used in providing consumer reports or consumer report information to a third party. A higher standard may be required for removal of a fraud alert.