Federal Register

Wednesday,
April 28, 2004

Part IV

Federal Trade Commission

16 CFR Parts 603, 613, and 614

Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act; Proposed Rule

FEDERAL TRADE COMMISSION

16 CFR Parts 603, 613, and 614

RIN 3084–AA94

Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act

AGENCY: Federal Trade Commission (FTC or the Commission).

ACTION: Notice of proposed rulemaking; request for public comment.

SUMMARY: The recently enacted Fair and Accurate Credit Transactions Act of 2003 (FACT Act or the Act), amending the Fair Credit Reporting Act (FCRA), establishes requirements for consumer reporting agencies, creditors, and others to help remedy identity theft. In this action, pursuant to authority in the Act, the Commission is proposing rules that would establish definitions for the terms ''identity theft'' and ''identity theft report;'' the duration of an ''active duty alert;'' and the ''appropriate proof of identity'' for purposes of sections 605A (fraud alerts and active duty alerts), 605B (consumer report information blocks), and 609(a)(1) (truncation of Social Security numbers) of the FCRA, as amended by the Act.

DATES: Written comments must be received on or before June 15, 2004.

ADDRESSES: Interested parties are invited to submit written comments. Comments should refer to ''FACTA Identity Theft Rule, Matter No. R411011'' to facilitate the organization of comments. A comment filed in paper form should include this reference both in the text and on the envelope, and should be mailed to the following address: Post Office Box 1030, Merrifield, VA 22116–1030. Please note that courier and overnight deliveries cannot be accepted at this address. Courier and overnight deliveries should be delivered to the following address: Federal Trade Commission/Office of the Secretary, Room H–159 (Annex J), 600 Pennsylvania Avenue, NW., Washington, DC 20580. Comments containing confidential material must be filed in paper form.

An electronic comment can be filed by (1) clicking on *http://www.regulations.gov*; (2) selecting ''Federal Trade Commission'' at ''Search for Open Regulations;'' (3) locating the summary of this Notice; (4) clicking on ''Submit a Comment on this Regulation;'' and (5) completing the form. For a given electronic comment, any information placed in the following fields—''Title,'' ''First Name,'' ''Last Name,'' ''Organization Name,'' ''State,'' ''Comment,'' and ''Attachment''—will be publicly available on the FTC Web site. The fields marked with an asterisk on the form are required in order for the FTC to fully consider a particular comment. Commenters may choose not to fill in one or more of those fields, but if they do so, their comments may not be considered.

Comments on any proposed filing, recordkeeping, or disclosure requirements that are subject to paperwork burden review under the Paperwork Reduction Act should additionally be submitted to: Office of Information and Regulatory Affairs, Office of Management and Budget, Attention: Desk Officer for the Federal Trade Commission. Comments should be submitted via facsimile to (202) 395–6974 because U.S. postal mail at the Office of Management and Budget is subject to lengthy delays due to heightened security precautions. Such comments should also be mailed to: FACTA Identity Theft Rule, Matter No. R411011, Post Office Box 1030, Merrifield, VA 22116–1030 or, if sent by courier or overnight delivery, delivered to: Federal Trade Commission/Office of the Secretary, Room H–159 (Annex J), 600 Pennsylvania Avenue, NW., Washington, DC 20580.

The Federal Trade Commission Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. All timely and responsive public comments, whether filed in paper or electronic form, will be considered by the Commission, and will be available to the public on the FTC Web site, to the extent practicable, at *www.ftc.gov*. As a matter of discretion, the FTC makes every effort to remove home contact information for individuals from the public comments it receives before placing those comments on the FTC Web site. More information, including routine uses permitted by the Privacy Act, may be found in the FTC's privacy policy, at *http://www.ftc.gov/ftc/privacy.htm*.

FOR FURTHER INFORMATION CONTACT: Naomi B. Lefkovitz, Attorney, Division of Planning and Information, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington, DC 20580. (202) 326–3228.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Introduction

The FACT Act was signed into law on December 4, 2003. Public Law 108–159, 117 Stat. 1952. Portions of the Act amend the FCRA to enhance the ability of consumers to resolve problems caused by identity theft. Section 111 of the Act adds a number of new definitions to the FCRA, including ''identity theft'' and ''identity theft report.'' The Act permits the Commission to further define the term ''identity theft,'' and requires the Commission to determine the meaning of the term ''identity theft report,'' although the Act does provide a minimum definition. Section 112 of the Act requires the Commission to determine the duration of an ''active duty alert,'' which the Act sets at a minimum of 12 months. Section 112 also requires the Commission to determine the ''appropriate proof of identity'' for purposes of sections 605A (fraud alerts and active duty alerts), 605B (consumer report information blocks), and 609(a)(1) (truncation of Social Security numbers) of the FCRA, as amended by the Act.

II. Overview of the Rules

A. Definition of Identity Theft

The Act confers certain rights on victims of identity theft designed to assist them in resolving problems caused by the identity theft (*see* sections 605A and 605B, and subsection 623(a)(B) of the FCRA).[1] In addition, the

[1] For example, an identity thief often will use victims' identifying information to open credit accounts on which he or she never pays the

Act creates certain requirements designed to reduce the occurrence of identity theft itself (*see* subsection 615(e) of the FCRA).[2] Thus, the definition of ''identity theft'' is critical because it defines the scope of fraudulent conduct that entities must take steps to prevent, and the definition determines who is, in fact, a victim entitled to take advantage of the rights conferred by the Act. The Commission believes that the definition should be sufficiently broad to cover all bona fide victims and conduct, but should be tailored to prevent individuals who are not identity theft victims from using the Act for unscrupulous purposes such as clearing negative, but legitimate, information from their credit records.

Section 111 of the Act defines the term ''identity theft'' to mean ''a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation.'' The Commission believes that additional definition of the term is warranted and proposes that the term ''identifying information'' have the same meaning as ''means of identification'' in 18 U.S.C. 1028(d)(7). The criminal code's definition of ''means of identification'' covers the appropriate range of identifying information and ensures that the term ''identity theft'' addresses the relevant permutations of fraud that might occur. It also ensures consistency with existing Federal law defining what constitutes identity theft, which promotes clarity and ease of application.

The Commission further proposes defining ''identity theft'' as a fraud which is attempted to be committed. Although identity thieves do not always succeed in opening new accounts, their attempts may be recorded as inquiries on victims' consumer reports. These inquiries may have an adverse affect on their credit scores,[3] therefore, victims should be entitled to take advantage of the Act to have these inquiries removed. In addition, victims who have learned of attempts by an identity thief and want to reduce the likelihood that the identity thief will succeed in opening new accounts, may want to place an ''initial fraud alert'' on their consumer reports.[4]

Finally, the Commission proposes to require that a person's identifying information must be used without lawful authority. Adding ''without lawful authority'' prevents individuals from colluding with each other to obtain goods or services without paying for them, and then availing themselves of the rights conferred by the Act to clear their credit records of the negative, but legitimate information.[5]

B. Definition of Identity Theft Report

Under section 111 of the Act, the Commission is required to determine the meaning of the term ''identity theft report.'' The Act provides that the term means ''at a minimum, a report—(A) that alleges identity theft; (B) that is a copy of an official, valid report filed by the consumer with an appropriate 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 (C) 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.''

Under the Act, an identity theft victim can use an ''identity theft report'' to mitigate a number of specific harms resulting from identity theft. First, under section 605A of the FCRA, victims can obtain an extended fraud alert, if they provide an ''identity theft report'' to consumer reporting agencies. An extended fraud alert is an alert placed in the consumer's file for seven years, which notifies users that the consumer may be a victim of fraud or identity theft and requires users to contact the consumer in person or by the contact method designated by the consumer before extending credit.[6] Thus, this fraud alert can prevent further occurrences of identity theft.

Second, under section 605B of the FCRA, victims can provide an ''identity theft report'' to consumer reporting agencies to have information resulting from identity theft that may adversely affect their credit histories blocked from their consumer reports. Notably, once an information furnisher is notified by a consumer reporting agency under section 605B of the FCRA that the consumer reporting agency is blocking information resulting from identity theft, the information furnisher must use reasonable procedures to prevent refurnishing this information, and cannot sell, transfer for consideration or place for collection debt resulting from the identity theft.[7]

Third, under subsection 623(a)(6)(B) of the FCRA, victims can provide an ''identity theft report'' directly to information furnishers to prevent these information furnishers from continuing to provide information resulting from identity theft to the consumer reporting agencies.

As a consequence of these uses, the identity theft report can be a powerful tool for identity theft victims in mitigating the harm resulting from identity theft. At the same time, it could provide a powerful tool for misuse, allowing persons to engage in illegal activities in an effort to remove or block accurate, but negative, information in their consumer reports.

In part to deter such possible misuse, the Act contains the requirement that the filing of the report be subject to criminal penalties for the filing of false information. As a further safeguard, the Act provides consumer reporting agencies and information furnishers with some ability to reject or reinstate a block or continue furnishing information. Specifically, a consumer reporting agency can decline or rescind a block if it reasonably determines that there is an error, a material misrepresentation of fact by the consumer, or the consumer obtained

charges. Eventually these accounts are reported as delinquent on the victims' credit records with the result that the victims may be denied the ability to obtain housing, job opportunities, or credit (or credit may be offered on less beneficial terms). To restore their records' accuracy, the victims need to be able to remove the fraudulent information from their consumer reports. The Act assists victims by enabling them to block the information resulting from identity theft from appearing on their consumer reports and to prevent information furnishers from continuing to furnish such information. (*See* sections 605B and 154(a) of the Act).

[2] Subsection 615(e) of the FCRA requires the Federal banking agencies, the National Credit Union Administration, and the Commission, jointly, to prescribe regulations with respect to ''red flags'' that financial institutions and creditors must implement in order to monitor for identity theft activity being perpetrated at their institutions.

[3] *Understanding Your Credit Score*, p. 14 at *http://www.myfico.com/Offers/myFICO_UYCS%20booklet.pdf*

[4] Under section 605A of the FCRA, ''initial fraud alerts'' which last for not less than 90 days, may be placed by consumers who can assert in good faith that they are or may be about to become victims of fraud or identity theft. Since users of consumers reports with these alerts who wish to extend credit (*see infra* n. 6) must take certain steps to verify the consumer's identity, these alerts can prevent identity thieves from opening new accounts.

[5] The Commission notes that the authority of a guardian, trustee, attorney-in-fact, or other person legally authorized to act on behalf of another does not extend to the commission of fraud. For example, in the case of a minor, the parent or guardian would have lawful authority to open a financial account *on behalf* of the minor, but no lawful authority to open the financial account *as* the minor, *i.e.*, pretending to be the minor. Thus, minors or other persons lacking legal capacity in such situations would still have rights under this Act.

[6] Extending credit is defined as establishing a new credit plan or extension of credit, other than under an open-end credit plan (as defined in section 103(i) of the Truth in Lending Act) or issuing an additional card on an existing credit account requested by a consumer, or granting any increase in credit limit on an existing credit account requested by a consumer.

[7] Subsections 623(a)(6)(A) and 615(f) of the FCRA.

possession of goods, services, or money as a result of the blocked transaction. *See* section 605B(c) of the FCRA. An information furnisher may continue to furnish the information if it knows or is informed by the consumer that the information is correct. *See* section 623(a)(6)(B) of the FCRA.

The Commission is concerned whether these safeguards provide sufficient protection from misuse. Traditionally, creditors and consumer reporting agencies have accepted police reports as a basis for blocking the record of an allegedly fraudulent transaction.[8] Under the Act, however, consumers could obtain an identity theft report by filing an allegation of identity theft with federal law enforcement agencies in a wholly automated manner, without any direct contact with a law enforcement officer.[9] Furthermore, the Commission anticipates that, over time, even local police departments that previously took in-person reports may increasingly turn to automated systems. If a consumer reporting agency or an information furnisher receives an identity theft report based on a copy of a law enforcement report filed by means of an automated system with little detail about the identity theft,[10] it may be difficult for it to determine whether the consumer presenting the identity theft report is a bona fide victim or an individual with delinquent debts seeking to clear his or her credit record. The potential for abuse of the credit reporting system is significant. At the same time, it is critical that victims be able to obtain the full benefits conferred by the Act in order to recover from the damage inflicted upon them by identity theft.

To address these concerns, the Commission is proposing to define "identity theft report" to include two additional elements. These elements are balanced to prevent abuse of the credit reporting system, without creating road blocks to a victim's recovery process or compensating for lax credit issuing practices. These additional safeguards work together to reinforce the existing protections of FCRA sections 605B(c)(1) and 623(a)(6)(B), *see supra*, which allow consumer reporting agencies and information furnishers leeway to reject requests for blocks.

First, the proposal would add to the definition of "identity theft report" a requirement that the consumer allege the identity theft with as much specificity as possible. The proposed rule provides four examples of types of information that the Commission considers helpful in investigating allegations of identity theft. These examples are for illustrative purposes only. Detailed information is critically important to law enforcement and, equally important, can help consumer reporting agencies and information furnishers distinguish between victims and those seeking to abuse the system. The Commission believes that this added specificity requirement will not disadvantage bona fide victims: they have to provide only what they know about the incident.

The proposal also would allow information furnishers or consumer reporting agencies to request additional information or documentation to help them determine the validity of the alleged identity theft. The request, however, must be reasonable, it must be for the purpose of determining the validity of the identity theft, and it must be made not later than five business days after the date of receipt of the copy of the law enforcement agency report or the request by the consumer for the particular service, whichever shall come later.[11] These limitations balance businesses' legitimate need to protect against fraud with bona fide victims' need to resolve the problems resulting from the crime without undue delay.

The proposed rule provides examples of when it may or may not be reasonable for information furnishers or consumer reporting agencies to request additional information or documentation. These examples are illustrative, and not exhaustive, and because they cannot take into account every unique circumstance, they are intended merely to provide general guidance. The examples demonstrate a range of law enforcement reports which a consumer might present to a consumer reporting agency or an information furnisher. In general, the request for additional information is intended to compensate for a report which does not rise to the level of the ideal law enforcement report (*i.e.*, a detailed report taken by a law enforcement officer face-to-face with the consumer which contains identifying or other contact information for the officer).

C. Duration of the Active Duty Alert

Section 112 of the Act provides certain consumers with the ability to place three types of alerts in their files maintained by a nationwide consumer reporting agency covered under the definition of section 603(p) of the FCRA. Two of the types of alerts are designed for consumers who are either victims of identity theft or who can assert in good faith that they are or may be about to become victims of fraud or identity theft.[12] The third type of alert is the

---

[8] Prior to the Act, creditors often requested a police report as proof that the consumer was a victim and not a delinquent debtor. A number of states, including California, Colorado, Idaho, and Washington had enacted laws which required consumer reporting agencies to block fraudulent information from consumer reports upon receipt of a police report. Presumably, police reports were relied upon because it was understood (perhaps not correctly in all cases) that in order to file a police report, an individual would need to go to the local police station and sit down with an officer, and that it was this face-to-face interaction with law enforcement that provided a sufficient level of deterrence against individuals who might seek to abuse the system.

The Act, however, expands valid law enforcement reports to include reports filed with state and federal law enforcement agencies as well as local law enforcement agencies. This expansion is a positive measure for victims because not all victims have been able to obtain reports from local police departments. The Commission found in its survey conducted by Synovate, in March-April 2003, that in the previous year, of the 26% of victims who sought to report their identity theft to a police department, 24% were not able to obtain a copy of a police report, *see* Synovate survey at *http://www.ftc.gov/os/2003/09/synovatereport.pdf* (data underlying the Synovate survey indicated that of this 24%, 9% of consumers did not know whether a police report was taken. Therefore, the Commission has inferred that these consumers did not obtain a copy of the report).

[9] Under these automated systems, consumers do not meet face-to-face with a law enforcement officer to provide the information about the identity theft. Consumers may mail in the reports, file them via the Internet, or provide the information over the telephone to staff who may not be criminal investigators.

Indeed, the Commission's own identity theft complaint collection system is an example of this kind of automated system and illustrates the possibility for abuse. Under the 1998 Identity Theft Assumption and Deterrence Act, Pub. L. No. 105–318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. 1028), Congress directed the Commission to collect complaints about identity theft from victims and to make those complaints available to other law enforcement agencies for use in their criminal investigations. In response, the Commission established its Identity Theft Data Clearinghouse, a centralized database that accepts identity theft complaints from consumers. The Commission's complaint system, however, 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. Now under the Act, 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).

[10] The section 111 definition requires only that an identity theft be alleged.

[11] A consumer reporting agency may accept an identity theft report for the purpose of placing an extended fraud alert without a request for additional information or documentation, but may want such additional information or documentation should the consumer, at a later date, request that certain information be blocked from appearing on his or consumer report.

[12] The first type is an "initial alert" which lasts for not less than 90 days and may be placed by

active duty alert. Military personnel who meet the definition of an active duty military consumer [13] are permitted to request it. This active duty alert was not designed to be a specific response to a threat of identity theft, but rather to be a preventive measure [14] for service members who are deployed in locations or situations in which they are unlikely to be able either to apply for credit or to monitor their financial accounts. The Act sets a minimum period of 12 months for the duration of the active duty alert, but requires the Commission to determine if this period should be longer.

The Commission considers that the duration of the active duty alert should be balanced between a length of time sufficient to meet the needs of the active duty military consumer as contemplated by the Act and a length of time that is not unduly burdensome to consumers [15] or creditors.[16] Although deployments for military personnel covered under the definition of an active duty military consumer are generally 12 months, some service members, such as members of the United States Air Force, may be deployed for shorter periods of time. Alternately, some reservists may spend up to 6 months prior to deployment in intensive training. This intensive training may take place in locations or situations similar to the deployment such that the reservists would have limited ability either to seek credit or to monitor their financial accounts. There also may be active duty military consumers who receive back-to-back or extended deployments. The Commission, however, understands that these consumers generally do not learn of their extended deployments until near the end of their initial deployments so it is impossible to anticipate who will receive them.

The Commission proposes that the duration of an active duty alert remain at the 12 months set forth by the Act. The Commission believes that 12 months will cover adequately the time period for which the majority of service members will be deployed. The Commission recognizes that 12 months may not sufficiently cover those active duty military consumers who receive extended deployments or who undergo intensive training prior to a 12-month deployment, however, these active duty military consumers may place another 12-month active duty alert after their first alert expires if they consider the additional period of protection to be necessary.[17] At the same time, the 12-month period will be too long for certain service members. The Commission seeks comment on whether it would be appropriate to establish a longer period of time for active duty fraud alerts.[18]

D. Appropriate Proof of Identity

Subsection 112(b) of the Act requires the Commission to determine what constitutes appropriate proof of identity for purposes of sections 605A (request by a consumer, or an individual acting on behalf of or as a personal representative of a consumer, for placing and removing fraud and active duty alerts), 605B (request by a consumer for blocking fraudulent information on consumer reports), and 609(a)(1) (request by a consumer for Social Security number truncation on file disclosures) of the FCRA, as amended by the Act.

In determining what should constitute ''appropriate proof of identity,'' the Commission has considered the risks associated with misidentifying a consumer. The two greatest apparent risks are that the file of the consumer making the request is confused with another consumer's file, or that a person pretending to be the consumer makes the request without the consumer's knowledge. The first instance can be prevented by requiring that consumers provide information sufficient to match them with their files. The second instance could be prevented by requiring an even greater degree of information sufficient to prove that the consumers are truly who they claim to be. Yet the information needed, in most instances to make an accurate file match, is relatively limited and easily produced by a consumer,[19] whereas the information necessary to prove that a consumer is who he or she claims to be could be substantially more burdensome for a consumer to produce, and might result in delays or even failure of the consumer to obtain the requested service, if the consumer reporting agency is unable ultimately to identify the consumer.

Therefore, the Commission proposes that the determination of ''appropriate proof of identity'' should balance the harm to the consumer that might arise from inadequate identification with the harm that might arise from delayed, or failed fulfillment of requested services due to greater levels of scrutiny. The Commission believes that the risk of consumer harm may differ depending on the service being requested or the method by which the request is made (*i.e.*, Internet, telephone, or mail), or may change over time, and that these risks may not apply equally to each consumer reporting agency. Consequently, the Commission believes that the standard of proof should be reasonably flexible to accommodate these differences, and that the consumer reporting agencies are in the best position to assess them. Thus, the proposed rule would require consumer reporting agencies to develop reasonable requirements to identify consumers in accordance with the risk of harm that may arise from a misidentification, but which, at a minimum, should be sufficient to match consumers with their files. The proposal provides examples of information for illustrative purposes only, that might constitute such reasonable requirements as follows:

(i) Consumer file match: The identification information of the victim including his or her full name (first,

---

consumers who can assert in good faith that they are or may be about to become victims of fraud or identity theft. The second type is an ''extended alert,'' which lasts for 7 years and may be placed by consumers who can allege that they are victims of identity theft. Users of consumers reports with these alerts who wish to extend credit must take certain steps to verify the consumer's identity. *See* section 605A of the FCRA.

[13] The term ''active duty military consumer'' means a consumer in military service who—

(A) is on active duty (as defined in section 101(d)(1) of Title 10 U.S.C.) or is a reservist performing duty under a call or order to active duty under a provision of law referred to in section 101(a)(13) of Title 10 U.S.C.; and

(B) is assigned to service away from the usual duty station of the consumer. FACT Act sec. 111, *codified at* FCRA sec. 603(q)(1), 15 U.S.C. 1681a(q)(1).

[14] Statement of Hon. Michael G. Oxley, Congressional Record, Extension of Remarks, E2513, December 8, 2002.

[15] Service members who return from their deployments prior to the expiration of the active duty alert may experience delays when attempting to enter into new credit transactions because of the presence of the alert. Although they can remedy this inconvenience by removing the alert, it is likely that removing an alert will be more difficult than placing an alert. *See infra* paragraph IID(1).

[16] The Act creates a new obligation for users of consumer reports that include these alerts. Users of consumer reports that include these alerts who are seeking to extend credit (*see supra* n.6) must use reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person seeking the credit. These procedures may include contacting the consumer by telephone. FACT Act sec. 112, *codified at* FCRA sec. 605A(h)(1), 15 U.S.C. 1681cA(h)(1).

[17] The Commission believes that because service members may go on deployments that trigger the elements of the definition of the term ''active duty military consumer'' several times during their service careers, they can place sequential active duty alerts. The Act is silent on this issue, but it would be illogical to read the Act otherwise.

[18] The Commission is of the view that the statutory language (''12 months or such longer period as the Commission shall determine'') requires a single, fixed period of time for the duration of active duty fraud alerts, and not a ''tiered'' system or other series of optional time periods.

[19] For example, such information may be limited to a name, date of birth, Social Security number, and current address.

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.

(ii) Additional proof of identity: copies of government issued identification documents, utility bills, and/or other current methods of authentication of a person's identity including, but not limited to answering questions to which only the consumer might be expected to know the answer.

(1) Fraud and Active Duty Alerts

It appears to the Commission that the appropriate proof of identity for placing a fraud or active duty alert may need to be only the information necessary for a consumer reporting agency to match consumers with their files. At this time, the Commission believes that the harm that would result from a delay in the placement of an alert would be greater than the harm resulting from an alert that is improperly placed in a consumer's file.[20] The consumer who has an alert improperly placed in his or her consumer file may experience some delay in obtaining an extension of credit while the user of the consumer report takes additional steps to verify the consumer's identity, however, the consumer can rectify the situation by removing the alert once he or she becomes aware of it. In comparison, the value of a functioning alert can be substantial as it has the potential to thwart identity theft before it begins or to prevent further damage.

Appropriate proof of identity also is required to remove an alert prior to its expiration. The principal risk of harm in this situation is that someone other than the consumer removes the alert. For example, an identity thief might seek to remove an alert in order to gain access to the consumer's credit.[21] In this instance, a delay in the removal of an alert might be the lesser harm. Hence, appropriate proof of identity in the context of removing an alert may call for a greater level of scrutiny than merely the information necessary to match consumers with their files.

(2) Fraudulent Information Blocking

Under section 605B of the FCRA, consumers who want to block information resulting from identity theft on their consumer reports need to provide appropriate proof of identity to the consumer reporting agency. To block this information, however, a consumer also must provide an "identity theft report"[22] and identify the specific information to be blocked. Therefore, in applying the balancing test, the risk that the wrong information will be blocked or that information will be blocked by a person other than the consumer seems relatively small. Consequently, it seems reasonable that appropriate proof of identity in the context of blocking information resulting from identity theft may need to be only the information necessary for the particular consumer reporting agency to match consumers with their files.

(3) Social Security Number Truncation

Under section 609(a)(1) of the FCRA, consumers who request that the first five digits of their Social Security numbers be truncated when requesting a file disclosure must provide appropriate proof of identity to the consumer reporting agency. However, under section 610 of the FCRA, the consumer reporting agency already must require the consumer to furnish proper identification before making any file disclosures to the consumer pursuant to section 609. Because of this underlying identification requirement, the risk of misidentifying the consumer appears small enough such that increasing the level of scrutiny to allow the consumer to truncate his or her Social Security number on the disclosed file does not seem reasonable.

III. Invitation to Comment

The Commission invites interested members of the public to submit written data, views, facts, and arguments addressing the issues raised by this Notice. Written comments must be received on or before June 15, 2004. Comments should refer to "FACTA Identity Theft Rule, Matter No. R411011" to facilitate the organization of comments. A comment filed in paper form should include this reference both in the text and on the envelope, and should be mailed to the following address: Post Office Box 1030, Merrifield, VA 22116–1030. Please note that courier and overnight deliveries cannot be accepted at this address. Courier and overnight deliveries should be delivered to the following address: Federal Trade Commission/Office of the Secretary, Room H–159 (Annex J), 600 Pennsylvania Avenue, NW., Washington, DC 20580. If the comment contains any material for which confidential treatment is requested, it must be filed in paper (rather than electronic) form, and the first page of the document must be clearly labeled "Confidential."[23]

An electronic comment can be filed by (1) clicking on *http://www.regulations.gov;* (2) selecting "Federal Trade Commission" at "Search for Open Regulations;" (3) locating the summary of this Notice; (4) clicking on "Submit a Comment on this Regulation;" and (5) completing the form. For a given electronic comment, any information placed in the following fields—"Title," "First Name," "Last Name," "Organization Name," "State," "Comment," and "Attachment"—will be publicly available on the Commission Web site. The fields marked with an asterisk on the form are required in order for the Commission to fully consider a particular comment. Commenters may choose not to fill in one or more of those fields, but if they do so, their comments may not be considered.

Comments on any proposed filing, recordkeeping, or disclosure requirements that are subject to paperwork burden review under the Paperwork Reduction Act should additionally be submitted to: Office of Information and Regulatory Affairs, Office of Management and Budget, Attention: Desk Officer for the Federal Trade Commission. Comments should be submitted via facsimile to (202) 395–6974 because U.S. postal mail at the Office of Management and Budget is subject to lengthy delays due to heightened security precautions. Such comments should also be mailed to: FACTA Identity Theft Rule, Matter No. R411011, Post Office Box 1030 Merrifield, VA 22116–1030 or, if sent by courier or overnight delivery, delivered to: Federal Trade Commission/Office of the Secretary, Room H–159 (Annex J), 600 Pennsylvania Avenue, NW., Washington, DC 20580.

The Federal Trade Commission Act and other laws the Commission

[20] The Commission has not been made aware of any concern that under the consumer reporting agencies' current practice of placing fraud alerts, fraud alerts have been improperly placed or consumers would be harmed more by the improper placement than by a delay in their placement. The concept of the "active duty" alert did not exist prior to the Act.

[21] Currently, there is no evidence of such occurrences, but such a pattern might evolve, especially if fraud prevention efforts in other areas become more effective.

[22] Consumers must comply with certain requirements that are designed to ensure that only the true victims of identity theft obtain an identity theft report. *See* section 111 of the Act.

[23] Commission Rule 4.2(d), 16 CFR 4.2(d). The comment must be accompanied by an explicit request for confidential treatment, including the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. The request will be granted or denied by the Commission's General Counsel, consistent with applicable law and the public interest. *See* Commission Rule 4.9(c), 16 CFR 4.9(c).

administers permit the collection of public comments to consider and use in this proceeding as appropriate. All timely and responsive public comments, whether filed in paper or electronic form, will be considered by the Commission, and will be available to the public on the Commission Web site, to the extent practicable, at *www.ftc.gov*. As a matter of discretion, the Commission makes every effort to remove home contact information for individuals from the public comments it receives before placing those comments on the Commission Web site. More information, including routine uses permitted by the Privacy Act, may be found in the Commission's privacy policy, at *http://www.ftc.gov/ftc/privacy.htm*.

IV. Communications by Outside Parties to Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding from any outside party to any Commissioner or Commissioner's advisor will be placed on the public record. *See* 16 CFR 1.26(b)(5).

V. Paperwork Reduction Act

The Commission has submitted this proposed Rule and a Supporting Statement for Information Collection Provisions to the Office of Management and Budget (OMB) for review under the Paperwork Reduction Act (PRA), 44 U.S.C. 3501–3520. As required by the FACT Act, the proposed rule defines the term ''identity theft report.'' Under the Act, an identity theft victim can mitigate a number of specific harms resulting from identity theft by providing an identity theft report to consumer reporting agencies and information furnishers.

The Commission staff estimates the paperwork burden of the Act and proposed rule based on its knowledge of identity theft trends and a recent identity theft study report, *Federal Trade Commission—Identity Theft Survey Report* (Survey Report), prepared for the Commission by Synovate, and issued in September, 2003.[24] Overall, the Commission staff has estimated that the average annual burden during the three-year period for which OMB clearance is sought will be 459,000 burden hours. The estimated annual labor cost associated with these paperwork burdens is $7.89 million.

Increase in number of individuals who obtain identity theft reports. The Survey Report indicates that there are 9.91 million individuals victimized by identity theft each year. Survey Report at 7. Twenty-six percent of those individuals, or 2.577 million, contact a local law enforcement agency. *Id.* at 59.[25] Seventy-six percent of the 2.577 million, or 1.958 million, file a police report alleging identity theft. *Id.* Prior to the Act, creditors might request a police report as proof that the individual reporting identity theft was a victim and not a delinquent debtor. The Act and proposed rule's expanded definition of ''identity theft report'' will allow individuals to obtain law enforcement reports from State and Federal law enforcement agencies, as well as local law enforcement agencies. Thus, the number of individuals who ultimately obtain an identity theft report will likely increase because the proposed rule will facilitate a victim's ability to file a law enforcement report.

First, the Survey Report indicated that 618,000 victims who contacted local law enforcement did not obtain a copy of a police report.[26] Thus, staff estimates that the proposed rule will enable those victims who previously were unable to obtain reports with local law enforcement to now file reports with a State or Federal law enforcement agency. Second, 4.261 million victims currently contact an information furnisher.[27] Staff estimates, based on its knowledge of identity theft trends, that the proposed rule will result in an increase of 10% or 426,000 of these victims obtaining an identity theft report. Third, 646,000 victims do not take any action even though their information was used to open new accounts or to commit other frauds.[28] Staff estimates, based on its knowledge of identity theft trends, that the proposed rule would likely result in 75% or 485,000 of these victims obtaining identity theft reports. In sum, staff estimates that the proposed rule will increase by 1.529 million the number of individuals obtaining identity theft reports. (618,000 + 426,000 + 485,000).

Hours and Cost Burden. Staff estimates, based on the experience of the Commission's Consumer Response Center, that an individual will spend an average of 5 minutes finding and reviewing filing instructions, 8 minutes filing the law enforcement report with the law enforcement agency, and 5 minutes submitting the law enforcement report and any additional information or documentation to the information furnisher or consumer reporting agency, resulting in an average of 18 minutes for each identity theft report.[29] Thus, the annual information collection burden for the estimated 1.529 million new identity theft reports due to the proposed rule will be 459,000 hours. [(1.529 million × 18 minutes)/60 minutes]. At an average national wage for individuals of $17.18 per hour,[30] the proposed rule will impose an estimated $7.89 million labor cost burden on individuals who obtain identity theft reports. ($17.18 × 459,000 hours).

The Commission solicits comment on the paperwork burden that the proposed rules may impose to ensure that no additional burden has been overlooked. The Commission invites comments that also will enable it to: (1) Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information will have practical utility; (2) evaluate the accuracy of the Commission's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (3) enhance the quality, utility, and clarity of the information to be collected; and (4) minimize the burden of the collection of information on those who must comply, including through the use of appropriate automated, electronic, mechanical, or other technological techniques or other forms of information technology.

VI. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA), 5 U.S.C. 601–612, requires that the Commission provide an Initial Regulatory Flexibility Analysis (IRFA) with a proposed rule and a Final Regulatory Flexibility Analysis (FRFA), if any, with the final rule, unless the Commission certifies that the rule will not have a significant economic impact on a substantial number of small entities. *See* 5 U.S.C. 603–605.

The Commission does not anticipate that the proposed rules will have a significant economic impact on a substantial number of small entities.

---

[24] *See* Synovate survey at *http://www.ftc.gov/os/2003/09/synovatereport.pdf*.

[25] All calculations in this section have been rounded to the nearest thousand.

[26] *See* Survey Report at 59 (24% of the 2.577 million victims who contacted law enforcement did not obtain a copy of a police report, *see supra* n.8).

[27] *See* Survey Report at 50 (43% of all victims contact an information furnisher).

[28] The data collected in the survey indicates that these types of victims constitute 20% of the 3.23 million victims each year whose information is used to open new accounts or commit other frauds.

[29] These estimates take into account that the time required to file the report will vary depending on the law enforcement agency used by the individual.

[30] The Bureau of Labor Statistics reports an average wage nationally for individuals of $17.18 per hour.

The Act expressly mandates most of the proposed rules' requirements, and thus accounts for most of the economic impact of the proposed rules. The proposed rule to establish the duration of an active duty alert at 12 months has an indirect impact on nationwide consumer reporting agencies described in section 603(p) of the FCRA, which provide the alert to users of consumer reports, and on users of consumer reports who are seeking to extend credit to consumers.[31] The Commission believes that currently there are no nationwide consumer reporting agencies that are small entities (*i.e.*, with less than $6 million in average annual receipts).[32] The Commission has been unable to determine how many users of consumer reports who are seeking to extend credit to consumers are small entities. Although there may be a number of small entities among these users of consumer reports, and the economic impact of the proposed rule on a particular small entity could be significant, overall the proposed rule likely will not have a significant economic impact on a substantial number of small entities.

The proposed rule directing the consumer reporting agencies to develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity for purposes of sections 605A (consumer request for placing and removing fraud and active duty alerts), 605B (consumer request for blocking fraudulent information on consumer reports), and 609(a)(1) (consumer request for Social Security number truncation on file disclosures) of the FCRA only applies to the consumer reporting agencies. As discussed above, the Commission believes that currently there are no nationwide consumer reporting agencies that are small entities. The Commission, however, has been unable to determine how many other consumer reporting agencies are small entities. Although there may be a number of small entities among the other consumer reporting agencies, and the economic impact of the proposed rule on a particular small entity could be significant, overall the proposed rule likely will not have a significant economic impact on a substantial number of small entities. The minimal impact on consumer reporting agencies would likely consist of merely applying a reasonable flexibility to existing, customary requirements developed in the normal course of their activities to ensure that they are providing the service requested by the consumer correctly.

Accordingly, this document serves as notice to the Small Business Administration of the agency's certification of no effect. To ensure the accuracy of this certification, however, the Commission requests comment on whether the proposed rules will have a significant impact on a substantial number of small entities, including specific information on the number of entities in each category that would be covered by the proposed rules, the number of these companies that are "small entities,'' and the average annual burden for each entity. Although the Commission certifies under RFA that the rules proposed in this notice would not, if promulgated, have a significant impact on a substantial number of small entities, the Commission has determined, nonetheless, that it is appropriate to publish an IRFA in order to inquire into the impact of the proposed rule on small entities. Therefore, the Commission has prepared the following analysis:

A. Description of the Reasons That Action by the Agency Is Being Taken

The FACT Act permits or directs the Commission to adopt rules that would establish: (1) Definitions for the terms "identity theft'' and "identity theft report;'' (2) the duration of an "active duty alert;'' and (3) the appropriate proof of identity for purposes of sections 605A (fraud alerts and active duty alerts), 605B (consumer report information blocks), and 609(a)(1) (truncation of Social Security numbers) of the FCRA, as amended by the Act. In this action, the Commission proposes, and seeks comment on, rules that would fulfill the statutory authorization and mandates.

B. Statement of the Objectives of, and Legal Basis for, the Proposed Rule

The objective of the proposed rules is to establish: (1) Definitions for the terms "identity theft'' and "identity theft report;'' (2) the duration of an "active duty alert;'' and (3) the appropriate proof of identity for purposes of sections 605A (fraud alerts and active duty alerts), 605B (consumer report information blocks), and 609(a)(1) (truncation of Social Security numbers) of the FCRA, as amended by the Act. The proposed rules are authorized by and based upon sections 111 and 112 of the FACT Act, Public Law 108–159, 117 Stat. 1952.

C. Small Entities to Which the Proposed Rule Will Apply

As described above, the proposed rules apply to consumer reporting agencies, including agencies that are small entities, if any, and to users of consumer reports, including users that are small entities, if any. A precise estimate of the number of small entities that are consumer reporting agencies (with less than $6 million in average annual receipts) and users of consumer reports within the meaning of the proposed rules, however, is not currently feasible. The Commission, therefore, invites comment and information on this issue.

D. Projected Reporting, Recordkeeping and Other Compliance Requirements

The Commission has tentatively determined that with respect to small entities, if any, the proposed rules do not include a collection of information subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501; 5 CFR 1320). The Commission, however, seeks comment on any paperwork burden that the proposed rules may impose on small entities to ensure that no burden has been overlooked.

E. Duplicative, Overlapping, or Conflicting Federal Rules

The Commission has not identified any other Federal statutes, rules, or policies that would duplicate, overlap, or conflict with the proposed rules. The Commission invites comment and information on this issue.

F. Significant Alternatives to the Proposed Rule

The Commission is not, at this time, aware of what particular alternative methods of compliance may satisfy the statute and also reduce the impact of the proposed rules on small entities that may be affected by the rules. The nature and number of such entities, if any, is unclear. Therefore, the Commission seeks comment and information with regard to (1) the existence of small business entities for which the proposed rules would have a significant economic impact; and (2) suggested alternative methods of compliance that, consistent with the statutory requirements, would reduce the economic impact of the rules on such small entities. If the comments filed in response to this notice identify small entities that are affected by the rules, as well as alternative methods of compliance that would reduce the economic impact of the rules on such entities, the Commission will consider the feasibility of such alternatives and determine whether they should be incorporated into the final rules.

[31] *See supra* n.6.

[32] *See* 13 CFR 121.201 (Small Business Administration's Table of Small Business Size Standards).

VII. Questions for Comment on the Proposed Rule

The Commission seeks comment on all aspects of the proposed rules. Without limiting the scope of issues on which it seeks comment, the Commission is particularly interested in receiving comments on the questions that follow. Responses to these questions should include detailed, factual supporting information whenever possible.

A. Questions Relating to the Definition of Identity Theft

1. Does the term ''identity theft'' as defined by the Act need further definition? If so, why? If not, why not?

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)? If so, why? If not, why not?

3. Should the Commission add the element of ''attempt'' to the definition of the term ''identity theft?'' If so, why? If not, why not?

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?'' If so, why? If not, why not?

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?'' If so, why? If not, why not?

6. Are there additional elements that the Commission should add to the definition of the term ''identity theft?'' If so, what should these elements be? What would be the advantages or disadvantages of adding these elements?

B. Questions Relating to the Definition of Identity Theft Report

1. Does the term ''identity theft report'' as defined by the Act need further definition? If so, why? If not, why not?

2. Should the Commission define what is an ''appropriate law enforcement agency''? If so, why? If not, why not?

3. To deter abuse of the credit reporting system, the Act requires that an identity theft report be subject to criminal penalties for false filing and allows consumer reporting agencies and information furnishers to reject a block or continue furnishing information. How likely is it that these safeguards will deter abuse of the credit reporting system? Are these safeguards less likely to deter abuse when automated systems are available to generate reports? If so, why? If not, why not? Are there alternate ways to deter abuse other than what the Commission has proposed? What would be the advantages or disadvantages of these alternate approaches?

4. Are the examples provided by the Commission of when it may or may not be reasonable for information furnishers or consumer reporting agencies to request additional information or documentation useful? If so, why? If not, why not? Are there alternate examples that would be more useful? If so, what would be the advantages or disadvantages of these alternate examples?

C. Questions Relating to the Duration of Active Duty Alerts

1. Should the Commission maintain the duration of the active duty alert at the minimum statutorily determined length of 12 months as proposed? If so, why? If not, why not?

2. Should the Commission set an alternate length of time for the duration of the active duty alert? If so, what should the appropriate length of time be? What would be the advantages or disadvantages of this alternate approach?

3. What fraction of active duty military consumers is likely to find the 12 month duration too short to cover their entire deployment?

4. How difficult will it be for active duty military consumers who receive intensive training or extended deployments to place, or to have a personal representative place another active duty alert if their initial alert expires before the end of the term of their deployment?

D. Questions Relating to the Appropriate Proof of Identity

1. Should the Commission set specific standards for what constitutes appropriate proof of identity? If so, what should those standards be? What would be the advantages or disadvantages of this alternate approach?

2. Are the examples of information that might be required by consumer reporting agencies appropriate or inappropriate? Why? Is there alternate information that should be used for examples? If so, what should the alternate information be? What would be the advantages or disadvantages of this alternate approach?

3. Has the Commission adequately balanced the harm that might arise from the consumer being misidentified and the harm arising from delays in, or potentially failure to provide, the consumers' requests due to greater levels of scrutiny? If so, why, If not, why not? Are there other factors that the Commission should consider? If so, what are these factors? What would be the advantages or disadvantages of these other factors?

List of Subjects in 16 CFR Parts 603, 613, and 614

Consumer reporting agencies, Consumer reports, Credit, Fair Credit Reporting Act, Identity theft, Information furnishers, Trade practices.

Note: Before this proposed rule is adopted as final, FTC expects to publish a rule redesignating the current part 603 with a new part number.

Accordingly, for the reasons set forth in the preamble, the Commission proposes to add parts 603, 613, and 614 of title 16 of the Code of Federal Regulations as follows:

PART 603—DEFINITIONS

Sec.
603.1 [Reserved]
603.2 Identity theft.
603.3 Identity theft report.

Authority: Sec. 111, 117 Stat. 1954, Pub. L. 108–159 (15 U.S.C. 1681a).

§ 603.1 [Reserved]

§ 603.2 Identity theft.

(a) The term ''identity theft'' means a fraud committed or attempted using the identifying information of another person without 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)).

§ 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 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, 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.

(b) Examples of the specificity referenced in paragraph (a)(1) of this section are provided for illustrative purposes only, as follows:

(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 information known to the consumer about the identity theft.

(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.

(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 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.

PART 613—DURATION OF ACTIVE DUTY ALERTS

§ 613.1 Duration of active duty alerts.

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

Authority: Sec. 112(a), Pub. L. 108–159, 117 Stat. 1955 (15 U.S.C. 1681c–1).

PART 614—APPROPRIATE PROOF OF IDENTITY

§ 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:

(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 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.

Authority: Sec. 112(b), Pub. L. 108–159, 117 Stat. 1956 (15 U.S.C. 1681c–1).

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 04–9485 Filed 4–27–04; 8:45 am]

BILLING CODE 6750–01–P