Office of Thrift Supervision **January 4, 2005**

Department of the Treasury

Transmittal

TR-363

Federal Register, Vol. 69 No. 212, pp. 63922 - 63934 **Number TR-363**

The Federal Trade Commission (FTC) published the attached final rule in the *Federal Register* on November 3, 2004. The final rule, which became effective on December 1, establishes 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 Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA). FCRA sections 605A, 605B, and 609(a)(1) became effective on December 1.

■ For the reasons stated in the preamble, SBA amends 13 CFR part 105 as follows:

PART 105—STANDARDS OF CONDUCT AND EMPLOYEE RESTRICTIONS AND RESPONSIBILITIES

■ 1. The authority citation for part 105 continues to read as follows:

Authority: 5 U.S.C. 7301; 15 U.S.C. 634, 637(a)(18) and (a)(19), 642 and 645(a).

■ 2. Revise § 105.101 to read as follows:

§ 105.101 Cross-reference to employee ethical conduct standards and financial disclosure regulations.

In addition to this part, Small Business Administration (SBA) employees should refer to the Standards of Ethical Conduct for Employees of the Executive Branch at 5 CFR part 2635 and the regulations at 5 CFR part 2634 entitled, Executive Branch Financial Disclosure, Qualified Trusts and Certificates of Divestiture.

■ 3. Amend § 105.402 by revising paragraphs (b) (2) and (b) (3) and removing paragraph (b) (4) to read as follows:

§ 105.402 Standards of Conduct Counselors.

* * * * *

(b) * * *

(2) Monitor the Standards of Conduct Program within their assigned areas and provide required reports thereon; and

(3) Review Confidential Financial Disclosure reports as required under 5 CFR part 2634, subpart I, and provide an annual report on compliance with filing requirements to the SBA Standards of Conduct Counselor as of February 1 of each year.

* * * * *

Hector V. Barreto,

Administrator.

[FR Doc. 04–24498 Filed 11–2–04; 8:45 am]

BILLING CODE 8025–01–P

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: Final rule.

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 document, the Commission issues final rules to 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: *Effective Date:* This rule is effective on December 1, 2004.

ADDRESSES: Requests for copies of the Rule and the Statement of Basis and Purpose should be sent to the Commission's Public Reference Branch, Room 130, Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington, DC 20580. The complete record of this proceeding is also available at that address. Relevant portions of the proceeding, including the Rule and Statement of Basis and Purpose, are also available at the Commission's Web site, *www.ftc.gov.*

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:

Statement of Basis and Purpose

I. Introduction

The FACT Act was signed into law on December 4, 2003. Pub. L. 108–159, 117 Stat. 1952. Portions of the Act amend the FCRA to enhance consumers' ability to resolve problems caused by identity theft. Section 111 of the Act adds several 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.

The Commission published a Notice of Proposed Rulemaking and request for Public Comment (''NPRM'') in the **Federal Register** on April 28, 2004,[1] and the comment period closed on June 15, 2004. The Commission received forty-nine comments.[2] The commenters included the National Association of Attorneys General Executive Committee, consumer advocacy groups,[3] industry trade organizations,[4] three nationwide consumer reporting agencies,[5] financial institutions and other companies,[6] two

[1] Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity under the Fair Credit Reporting Act, 69 FR 23370 (proposed April 28, 2004) (to be codified at 16 CFR. parts 603, 613, and 614).

[2] The public comments relating to these rulemakings may be viewed at *http://www.ftc.gov/os/comments/factaidt/index.htm.* The Commission considered all comments timely filed, *i.e.*—those received on or before the close of the comment period on June 15, 2004. As a matter of discretion, the Commission also considered comments that were filed after the close of the comment period. Citations to comments filed in this proceeding are made to the name of the organization (if any) or the last name of the commenter, and the comment number of record. Comment number may appear as all numeric characters—*e.g.*, #000031 (indicating a comment received by paper or electronic mail), or as numeric characters preceded by ''EREG''—*e.g.*, ''EREG–000031'' (indicating a comment received through www.regulations.gov).

[3] Consumers Union submitted a comment on behalf of 11 organizations. Consumer advocacy groups commenting included Consumer Action, Consumer Federation of America, Consumers Union, Electronic Privacy Information Center, Identity Theft Resource Center, National Association of Consumer Advocates, National Consumer Law Center, National Council of La Raza, Privacy Rights Clearinghouse, Privacy Times, and U.S. Public Interest Research Group (US–PIRG).

[4] In addition to Consumer Data Industry Association (CDIA)—the trade association that represents the nationwide consumer reporting agencies and a variety of other consumer reporting agencies—the Commission received comment on the proposed rule on behalf of a number of trade organizations representing a variety of industries and concerns. These included ACA International (representing debt collection agencies and other accounts receivable professionals), American Bankers Association, American Financial Services Association (representing companies primarily engaged in the business of providing consumer credit), America's Community Bankers, Credit Union National Association (CUNA), Coalition to Implement the FACT Act (representing trade associations and companies that furnish, use, collect, and disclose consumer information), Consumer Bankers Association, Independent Community Bankers of America, National Automobile Dealers Association, National Business Coalition on Privacy and E-Commerce (representing diverse companies interested in national policy on privacy and electronic commerce issues), Michigan Credit Union League, National Retail Federation, Pennsylvania Credit Union Association, and the Financial Services Roundtable.

[5] Equifax Information Services LLC, Experian Information Solutions, Inc., and Trans Union LLC.

[6] These included Bank of America, Bank One Corporation, BMO Financial Group, Boeing Employees' Credit Union, Capital One Financial Corporation, Countrywide Home Loans, Fifth Third

of the four military service branches,[7] consumers,[8] and the National Notary Association, a professional trade organization. Unless specifically modified in this document, all of the analysis accompanying the proposed rules in the NPRM is adopted and incorporated into this Statement of Basis and Purpose for the final rules.

II. Analysis of the Comments Received

A. Section 603.2: Identity Theft

The definition of ''identity theft'' triggers important duties for businesses and important rights for consumers under the FACT Act and the FCRA. For example, it defines the scope of fraudulent conduct that businesses must take steps to prevent, and it determines who is a victim entitled to take advantage of the rights conferred by the Act. Section 111 of the Act defines the term ''identity theft'' as ''a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation.'' In the NPRM, the Commission proposed to further define the term ''identity theft'' [9] so it would be sufficiently broad to cover all bona fide victims and conduct, and also help prevent credit repair fraud.[10]

1. Attempted Fraud

In the NPRM, the Commission proposed adding ''attempt to commit fraud'' to the definition. Although identity thieves do not always succeed in opening new accounts, their attempts to do so may be recorded as inquiries on victims' consumer reports, which may adversely affect the victims' credit scores. Victims who learn of attempts by an identity thief should be entitled to take advantage of the Act to place extended fraud alerts and block fraudulent inquiries. To block these inquiries under section 605B of the FCRA and to obtain an extended fraud alert, victims need to be able to obtain an identity theft report for which they need to be able to allege an identity theft. For these reasons, the Commission proposed adding ''attempt to commit fraud'' to the definition. Although a number of commenters supported this position,[11] a number of commenters also opposed including ''attempt'' in the definition of ''identity theft.'' These commenters made three principal arguments.

First, some commenters argued that it is not necessary for the Commission to include ''attempt'' in the definition of ''identity theft'' to enable consumers to remove fraudulent inquiries from their consumer reports because these victims can dispute inaccurate information in consumer reports with section 611 of the FCRA instead of section 605B.[12] If the Commission were to eliminate ''attempt'' from the definition, it would be creating separate processes for handling fraudulent tradelines and handling fraudulent inquiries under the FCRA. No commenter indicated why fraudulent inquiries should be treated differently from fraudulent tradelines. Further, the section 611 dispute process may not provide an adequate means of removing inquiries. Because section 611 relies on consumers' ability to produce ''relevant documentation,'' [13] it is best suited to addressing inaccurate information that results from errors where consumers can provide records showing that they have, for example, paid their debts. Victims of identity theft, however, have no records showing that they did not open an account and therefore, incurred no debts. Section 605B, however, enables victims to use a law enforcement report as the basis of their proof of the identity theft to block information specifically resulting from identity theft from appearing on their consumer reports. Thus, section 605B is designed specifically to help identity theft victims correct information in their consumer reports that results from fraudulent activity, whereas section 611 is not specifically tailored for identity theft victims. Thus, the Commission sees no reason why consumers with inquiries resulting from attempted fraud should be barred from using this process.

Second, commenters stated that it was not necessary for the Commission to include ''attempt'' to assist in the placement of fraud alerts because consumers do not need to be actual victims of identity theft to place an initial fraud alert.[14] The Commission agrees that consumers will not need to prove identity theft to place an initial fraud alert. The Commission, however, is concerned that in situations where the identity thief continues to attempt to perpetrate frauds, these victims may wish to place an extended fraud alert. Under section 605A of the FCRA, such victims will need an identity theft report alleging an identity theft to obtain the extended fraud alert. An extended fraud alert under these circumstances will alert businesses of the need to take greater precautions and help to prevent losses.

Finally, commenters argued that including ''attempt'' would divert resources that could be better used to assist victims whose information has been actually misused.[15] It is not clear

---

Bank, Household International, Inc., Juniper Bank, Keycorp, MasterCard International, MBNA America Bank, N.A., Navy Federal Credit Union, Nissan Motor Acceptance Corp., Sprint Corporation, Teachers Federal Credit Union, Visa U.S.A., Inc., Wells Fargo and Company, and Wilshire Credit Corporation.

[7] These were the Office of the Judge Advocate General, Department of the Navy and the United States Marine Corps.

[8] These included Beverly Davis, Mike Heinemann, Robert Pinheiro, Abbi Sexton, and Charles Nichols.

[9] 69 FR 23377. In the NPRM, the Commission defined the term ''identity theft'' to mean 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)).

[10] *Id.* at 23371.

[11] *See, e.g.*, Keycorp #EREG–000007 (''We support the inclusion of attempted theft in the definition of 'identity theft' under the Act. Allowing a consumer to file an initial identity theft report based on an attempted ID theft affords greater protection for consumers and users of consumer reports.''); Equifax Information Services, LLC #000023 (''Since an initial fraud alert may be placed on a consumer's file by a consumer reporting agency when the consumer has a suspicion that he or she 'is about to become' a victim of fraud, including 'attempt' to commit fraud as part of the definition is a logical and useful extension.''); and Teachers Federal Credit Union #EREG–000009 (''Yes, attempts to commit frauds should be included in the definition, since fraud attempts may have an adverse affect on a victim's credit report/score.'').

[12] *See, e.g.*, MasterCard International #000025 (''We note that consumers who are victims of attempted identity theft have the ability to correct their consumer reports using the dispute process already provided for in the FCRA. Thus, an expanded definition of 'identity theft' is not necessary to provide victims a remedy to correct data on a consumer report.'').

[13] Section 611 of the FCRA, 15 U.S.C. 1681i.

[14] *See, e.g.*, MasterCard International #000025 (''The Commission also suggests that a broad definition is necessary because 'victims who have learned of attempts by an identity thief and want to reduce the likelihood that the identity thief will succeed in opening new accounts may want to place an 'initial fraud alert' on their consumer reports.' We respectfully note that the statute does not require a consumer to be a victim of 'identity theft' in order to place an initial alert in the consumer's file. All that is necessary to place an initial alert in the file is for the consumer to assert 'in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime.' We believe that a consumer who has been a victim of attempted identity theft could make such an assertion regardless of whether 'identity theft' were to also mean 'attempted identity theft.' '').

[15] *See, e.g.*, Wells Fargo and Company #000015 (''We are concerned that defining 'identity theft' to

Continued

how the inclusion of ''attempt'' would create such economic hardship as to cause private entities to reallocate resources designated for assisting victims; the provisions of the Act that implicate ''attempt'' either do not affect most private entities or would seem to assist in the prevention of identity theft. For instance, creditors must take certain steps to verify consumers' identities when fraud alerts appear on consumer reports.[16] Such verification would seem worthwhile to prevent identity theft for consumers and financial institutions. Notably, consumer reporting agencies, who will be the only private entities obligated to place fraud alerts and block inquiries, either supported the inclusion of ''attempt'' or did not comment.[17] Similarly, inclusion will not result in increased processing of identity theft reports by information furnishers because no accounts will have been opened.

Accordingly, the Commission retains ''attempt'' in the definition of identity theft.

2. Identifying Information

In the NPRM, the Commission proposed that ''identifying information'' should have the same meaning as ''means of identification'' found in the federal criminal code.[18] This would ensure that the term ''identity theft'' addressed the potential permutations of identity fraud that might occur. It would also provide consistency with the federal criminal law. A number of commenters supported the Commission's proposal.[19] However, because ''means of identification,'' as defined in the criminal statute, includes check routing, credit card, and debit card numbers, a number of commenters were concerned that the proposed rule would cover too broad a range of frauds, in particular, unauthorized use of a consumer's existing accounts.[20]

For example, some commenters argued against including unauthorized use of accounts in the definition of ''identity theft'' because other federal laws provide victims with sufficient protection.[21] While other federal laws may provide victims with the means to redress certain aspects of injuries resulting from the unauthorized use of an account, these other laws do not necessarily address all aspects of their injuries. For example, under the Fair Credit Billing Act,[22] victims can dispute unauthorized credit card transactions on their billing statement, but if the debts resulting from the disputed charges appear on their consumer reports as delinquent,[23] or if the victims need to obtain related transaction records to assist in proving their claim,[24] victims may need to apply the rights provided by the FACT Act. The Commission expects that victims of unauthorized account use will continue to resolve their problems under other federal laws as applicable, but they also may need and are entitled to the protections provided by the Act.

Commenters also were concerned that including unauthorized use of a consumer's existing accounts would encourage abuse of the credit reporting system.[25] The Commission recognizes the concern that the Act, in creating new tools to assist victims in recovering from identity theft (*e.g.*, by enabling them to use the ''identity theft report'' to block the reporting of fraudulent debts in their consumer reports theft report,'' *see infra* II.B.), may give unscrupulous individuals a new, or alternative means to attempt to exploit the credit reporting system. The Commission, however, finds that the definition of ''identity theft report'' (*see infra* II.B.) provides consumer reporting agencies and information furnishers with adequate means to distinguish between bona fide identity theft victims and consumers attempting to defraud the system. The Commission has concluded, therefore, that the possibility of limiting the potential for abuse that might arise from narrowing the definition of identity theft is outweighed by the need to provide bona fide victims of unauthorized account use with the same rights accorded victims of other forms of identity theft under the FCRA.

Accordingly, except for a technical change discussed in paragraph II.A.4, the Commission defines ''identifying information'' to have the same meaning as ''means of identification'' found in 18 U.S.C. 1028(d)(7).

3. Lawful Authority

In the NPRM, the Commission proposed that the definition of identity theft require that a person's identifying information must be used ''without

include ''attempted'' fraud would greatly expand the scope of conduct that entities must take steps to prevent and would significantly increase the number of consumers authorized to take advantage of the rights that the FCRA confers upon identity theft victims. Expanding the definition of identity theft beyond the traditional notion of an individual opening an account or obtaining a loan in another person's name would divert significant resources away from actual identity theft and its victims in order to assist those who have avoided any meaningful harm of identity theft. If a fraud is attempted but not completed, the system will have averted identity theft and the consumer will have suffered little, if any, harm. Any harm that the consumer will have suffered can be, or already will have been, adequately addressed.'').

[16] Section 605A of the FCRA, 15 U.S.C. 1681c–1.

[17] *See, e.g.*, Consumer Data Industry Association #000012 (''CDIA agrees with the Commission that, in order to trigger the important FCRA rights of potential identity theft victims and to enable them to avoid being actual identity theft victims, the definition should cover an attempted fraud, as well as the actual offense.''); Experian Information Solutions #000009 (''The definition captures the appropriate elements; it includes (a) a fraud that is attempted or committed, (b) using 'identifying information' of another, and (c) without lawful authority.''); and Equifax Information Services, LLC #000023 (''Since an initial fraud alert may be placed on a consumer's file by a consumer reporting agency when the consumer has a suspicion that he or she 'is about to become' a victim of fraud, including 'attempt' to commit fraud as part of the definition is a logical and useful extension.'').

[18] ''Identity theft'' is defined in 18 U.S.C. 1028(a)(7) and ''means of identification'' is defined in 18 U.S.C. 1028(d)(7).

[19] *See, e.g.*, Office of the Judge Advocate General, Department of the Navy #000011 (''As the Commission points out, 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. Additionally, [sic] the Commission accurately states, it ensures consistency with existing Federal law defining what constitutes identity theft, which promotes clarity and ease of application.'') and Experian Information Solutions #000012 (''Experian supports this definition as well; it encompasses the different kinds of information that could be used to commit an identity theft.'').

[20] *See, e.g.*, National Retail Federation #000005 (''We would strongly urge the Commission to limit its definition of an identity theft to those situations in which the perpetrators have actually assumed someone else's identity, procured a new line of credit and used that credit in the individual's name. We urge this formulation to distinguish true ID Theft from 'attempted' identity theft or from situations involving 'unauthorized use.' '').

Consumers themselves, however, consider that unauthorized use of their accounts is a form of identity theft based on the fact that they file complaints in the Commission's identity theft complaint database about such unauthorized use. *See http://www.consumer.gov/idtheft/charts/CY2002OverallCharts.pdf* for examples of the statistical breakdown of consumer identity theft complaints to the Commission.

[21] *See, e.g.*, Coalition to Implement the FACT Act #000019 (''Not only are there already provisions in existing law, such as under the Truth in Lending Act and the Electronic Fund Transfer Act, to protect consumers who are victims of crimes such as account fraud, but we do not believe it would benefit victims of true identity theft to dilute industry's efforts by giving victims of less debilitating crimes equal priority as identity theft victims.'').

[22] 15 U.S.C. 1666–1666j.

[23] *See* section 605B of the FCRA for the right to block information resulting from identity theft from consumer reports. 15 U.S.C. 1681c–2.

[24] *See* section 609(e) of the FCRA for the right to obtain identity theft related transaction records. 15 U.S.C. 1681g.

[25] *See, e.g.*, Wells Fargo and Company #000015 (''We also believe that inclusion of traditional debit and credit card fraud in the definition of 'identity theft' will significantly increase claims of identity theft, fraud alerts and requests to block information. A significant increase in claims of this type (many of which may be marginal or even untrue) could impact the integrity of the entire information reporting system.'').

lawful authority.'' This definition was designed to prevent individuals from colluding to obtain goods or services without paying for them and then using the rights conferred by the Act to clear their credit records of the negative, but legitimate, information. Most commenters supported the Commission's addition, although some asked for additional clarification.

Some commenters suggested that ''without lawful authority'' might not fully prevent collusion.[26] These commenters appear to argue that, because no one can ''lawfully'' authorize an illegal act, a person might give another person permission to use his or her identifying information knowing that the recipient would use such information to commit fraud, and then later allege ''identity theft'' because he never gave ''lawful authority'' to use the information to commit fraud.[27] The Commission doubts that the inability to ''lawfully'' authorize a fraudulent act would provide a justification for alleging identity theft in such circumstances. Nevertheless, to avoid any such result, the Commission is deleting the term ''lawful'' from the final Rule. Thus, the final Rule states that ''identity theft'' means ''a fraud committed * * * using the identifying information of another person without authority.'' The Rule is intended to apply to one person's using the identifying information of another person without that person's permission or approval.

In the NPRM, the Commission had asked for comment on whether the definition of ''identity theft'' should include a requirement that a person's identifying information be used without the person's knowledge, to address concerns with collusion. The Commission received few responsive comments, and although such a requirement could address collusion, it would create problems for bona fide victims who may know that their identifying information is in the process of being used, but cannot stop the use. Thus, the Commission has determined not to include ''without knowledge'' in the definition of identity theft.

More broadly, some commenters were concerned that adding ''without lawful authority'' would increase the difficulty of recovery for certain victims such as minors.[28] In the NPRM, the Commission stated that parents who use their minor children's identifying information purporting to be the minors are not exercising lawful authority. Lawful authority, or authority alone, allows parents to use their minor children's identifying information on behalf of the minors, but only when acting in the capacity as the parent. Minors whose parents have misused their identifying information by purporting to be the minors will, therefore, be able to assert that their parents acted without authority and will be entitled to all of the identity theft protections under the FCRA.

Some commenters suggested a clarification that presumed authority if the consumer refused to pursue prosecution.[29] Although refusal to prosecute may be a factor in considering whether an unauthorized use of a person's identifying information has occurred, the Commission does not believe that it constitutes *prima facie* evidence of a grant of authority. Accordingly, the Commission declines to include a person's refusal to prosecute the user of the person's identifying information in the final rule.

4. Additional Changes

One commenter suggested that the Commission amend paragraph (b)(4) (see n. 9) to clarify that identifying information includes credit card and other account identification numbers by incorporating the language referenced in 18 U.S.C. 1029(e) into the final rule.[30] The Commission considers that including the specific language of 18 U.S.C. 1029(e) would add unnecessary verbiage to the rule and that the Commission can use other means to publicize the concept that credit card account numbers are included in the definition. For example, the Commission previously addressed (*see, supra* II.A.2) the fact that unauthorized account use is part of the definition of identity theft, and the Commission will highlight this fact in any educational materials it develops.

Finally, the Commission has corrected a drafting error made in clarifying the term ''identifying information.'' In paragraph (b), the Commission has replaced the clause ''to identify a specific individual'' with ''to identify a specific person'' to conform the elements of ''identifying information'' with the definition of ''identity theft'' in the Act, which uses the term ''person.''

Except for this technical change and the removal of the word ''lawful,'' the Commission adopts the definition of ''identity theft'' without modification.

B. Section 603.3: Identity Theft Report

Under section 111 of the Act, the Commission is required to determine the meaning of the term ''identity theft report,'' using as the foundation a minimum definition set forth in the Act.[31] Consumers can use the identity

[26] *See, e.g.*, Consumer Bankers Association #000007 (''The FTC states that 'adding ''without lawful authority'' [to the definition] prevents individuals from colluding with each other to obtain goods or services without paying for them, and then' attempting to allege that it is the result of identity theft. CBA applauds the FTC for addressing this important issue. We do not believe that consumers who benefit from a transaction should be able to claim that the transaction is the result of identity theft. Therefore, we urge that this concept be retained. However, we also ask the FTC to clarify this issue in the Final Rule. In particular, as the definition is drafted, it is not clear whether the modifier 'without lawful authority' would achieve the FTC's objective because a fraud is already generally an act committed without lawful authority.'').

[27] *Id.*

[28] *See, e.g.*, Consumers Union #EREG–000002 (''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.'').

[29] Consumer Data Industry Association #000009 (''CDIA agrees that an important element of the definition of identity theft is that the person's identifying information is used without lawful authority. As the Commission observes, individuals, such as guardians and attorneys-in-fact, may have lawful authority to use another's identifying information and may misuse that information to commit fraud. CDIA's members have experienced situations where consumers appear to have colluded with family members or friends to perpetrate a fraud or attempted fraud using their own identifying information. In those instances, the consumer refuses to prosecute the perpetrator of the fraud or attempted fraud. For that reason, CDIA believes that the final rule should provide that a consumer's refusal to prosecute the perpetrator of an identity theft is prima facie evidence that the consumer's identifying information was used with the consumer's lawful authority and thus does not involve identity theft.'').

[30] Consumer Data Industry Association #000009 (''As a result of incorporating the U.S. Code definition into the proposed rule, the rule's definition of identity theft could include the authorized [sic] use of a credit card, PIN or similar access device. CDIA understands that the Commission intends this result. However, affected industry members may not associate the crime of identity theft with the fraudulent use of a credit card number without identifying information. For that reason, in order to facilitate compliance, CDIA suggests that the final rule's definition of identifying information incorporate the current U.S. Code definition of 'any telecommunication identifying information or access device.' The final rule could also provide that the definition would include the U.S. Code definition as it may be amended, to reflect changes in technology.'').

[31] Under the Act, an identity theft report is, ''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,

Continued

theft report to block information resulting from identity theft from their consumer reports [32] and prevent information furnishers from refurnishing such information,[33] as noted in the NPRM. The Commission is concerned that the identity theft report might be misused by some to attempt to remove accurate, but negative, information from their consumer reports, notwithstanding the Act's requirement that the filing of the report be subject to criminal penalties for the filing of false information.[34] Because certain law enforcement agencies, including most federal agencies, allow consumers to file law enforcement reports through an automated system (*i.e.*, the report can be filed by mail, telephone, or via the Internet, instead of in a face-to-face interview with a law enforcement officer), the Commission is concerned that consumers using an automated means might have less compunction about filing a false report. Moreover, because consumer reporting agencies and information furnishers most likely will receive and be required to act upon the law enforcement report before the identity theft complaint is fully investigated by the law enforcement agency, they will be faced with the initial responsibility for determining the legitimacy of an identity theft claim.[35]

For these reasons, the Commission's proposal allowed consumer reporting agencies and information furnishers to investigate identity theft claims much to the same extent that they could prior to the Act. At the same time, the Commission wanted to ensure that bona fide victims could resolve their identity theft problems without undue delay or burden. The Commission's proposal, with specific limitations, allows consumer reporting agencies and information furnishers to make requests for information and documentation in addition to the law enforcement report to verify the identity theft claim, and to require that consumers allege the identity theft with as much specificity as possible.[36] The Commission also proposed some examples of when it would or would not be reasonable to request additional information or documentation. While a few commenters unreservedly supported the Commission's proposal,[37] as outlined below, most commenters had concerns about some aspect of the Commission's proposal.

Although many commenters were concerned about the possibility of misuse of the identity theft report, they felt that the Commission's proposed remedies were not sufficient to deter this potential problem.[38] Commenters suggested ways in which the rule could better address this concern. For example, some commenters wrote that the Commission should limit the type of law enforcement agency with which a report about identity theft could be filed by further defining what constitutes an ''appropriate'' law enforcement agency. Specifically, some commenters suggested narrowing the term to exclude law enforcement agencies that enforce laws unrelated to identity theft on the grounds that they are unlikely to investigate any reports of identity theft which they receive, thus encouraging the filing of false reports.[39] Other commenters felt that law enforcement agencies with automated systems should not be considered ''appropriate.'' [40] Finally, a number of commenters thought that the Commission should clarify that the Commission itself is not an appropriate law enforcement agency in part because it lacks criminal arrest authority.[41]

After considering these comments, the Commission has determined that it is not necessary to limit further the law enforcement agencies with which identity theft victims can file a report. First, the Commission does not find that restricting law enforcement agencies to those that enforce specific identity theft laws would provide meaningful guidance because identity theft can take many forms and can be prosecuted under many different laws.[42] Rather, the

if, in fact, the information in the report is false.'' 15 U.S.C. 1681a(q)(4).

[32] Section 605B of the FCRA, 15 U.S.C. 1681c–2.

[33] Section 623(a)(6)(B) of the FCRA, 15 U.S.C. 1681s–2(a)(6)(B).

[34] 69 FR 23371.

[35] As further protection against abuse of the credit reporting system, the Act also provides the consumer reporting agencies and information furnishers with some ability to reject or reinstate a block or continue furnishing information (*see* sections 605B(c) and 623(a)(6)(B) of the FCRA, 15 U.S.C. 1681c–2(c) and 15 U.S.C. 1681s–2(a)(6)(B)). In practice, it may be difficult for the consumer reporting agencies or information furnishers to make such determinations without an investigation of the claim of identity theft. This investigation may be difficult to conduct without the cooperation of the consumer making the claim.

[36] 69 FR 23372. The definition proposed in the NPRM:

(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 (2) or the request by the consumer for the particular service, whichever shall be the later.

[37] *See, e.g.*, Independent Community Bankers of America #EREG–000004 (''The ICBA agrees that it is appropriate that credit reporting agencies and information furnishers have the authority to require as much specificity as possible when investigating an allegation of identity theft. To begin with, this will help discourage fraudulent claims of identity theft and abuse of the system, a step that is especially important since, as noted above, Congress created serious remedies for a serious problem. Second, greater specificity will help information furnishers and credit reporting agencies better identify the actual fraud that should be blocked on a credit report.'').

[38] *See, e.g.*, American Financial Services Association #000010 (''AFSA appreciates the Commission's effort to carefully balance the important considerations underlying the FACTA identity theft provisions * * * as the Commission recognizes in its Supplementary Information accompanying the Proposed Rule, identity theft reports '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 from their consumer reports.' [Footnote 2: 69 Fed. Reg. 23,371.] AFSA is concerned that the Proposed Rule has not fully addressed this risk identified by the Commission and that, as written, the Rule may allow the unscrupulous to turn a system intended to protect consumers into a system that could be easily used to deceive and defraud creditors and other users of consumer report information.'').

[39] *See, e.g.*, Consumer Bankers Association #000007 (''For example, the statute would appear to prohibit the filing of an identity theft report with the Federal Communications Commission (''FCC''), because an agency charged with enforcing several different laws unrelated to identity theft would clearly not be an appropriate recipient of a report alleging identity theft. Not only can the FCC do very little about investigating the identity theft, but the FCC is unlikely to spend a lot of resources to determine whether the consumer has lied in the report.'').

[40] *See, e.g.*, Boeing Employees Credit Union #000002 (''We do not agree with the automated method of reporting identity theft. Allowing the reporting to be a faceless transaction with zero law enforcement involvement makes it extremely convenient for someone to falsify a report. In our opinion, to qualify for these protections, the consumers must provide adequate proof of fraud in person.'').

[41] *See, e.g.*, American Bankers Association #EREG–000034 (''Complaints filed with the Commission's Identity Theft Data Clearinghouse should be excluded, unless the Commission has authority to arrest a person filing a false report.'').

By contrast, the National Association of Attorneys General (#000008) suggested that the Commission explicitly include itself as an agency with which victims can file identity theft complaints in the final rule. The Commission considers that the final rule is clear that victims may submit reports to any federal law enforcement agency which accepts identity theft complaints. Therefore, although Congress opted to name the United States Postal Inspection Service in the definition of ''identity theft report,'' it is unnecessary to name the Commission or any other federal agency specifically.

[42] A law enforcement agency may derive its authority to investigate identity theft cases not from a specific law criminalizing identity theft, but from a law criminalizing bank fraud, for example.

Commission notes that consumer reporting agencies and information furnishers may take into account whether the agency with which the law enforcement report was filed appears to have been chosen for the purpose of avoiding inquiry into the identity theft when determining whether to request additional information or documentation to assess the validity of the identity theft claim.

Second, the Commission notes that some victims are faced with police departments that will not take identity theft complaints. This problem, combined with the fact that most federal and some state law enforcement agencies use automated systems to take reports means that excluding law enforcement agencies that take automated reports would unduly burden victims of identity theft. Finally, the Commission is not convinced that excluding the Commission's complaint intake system would diminish the risk of false filings, because the Commission, like any other law enforcement agency, can take steps to pursue any evidence of false filings.[43]

On a different issue, certain commenters raised concerns about the meaning of an ''official, valid report.'' Some requested that the Commission clarify this concept. In order for the report to be considered official and valid, others wanted the report form to state that criminal penalties apply to false statements.[44] The Commission does not find the term ''official, valid report'' to be ambiguous. Further, if the consumer reporting agencies or information furnishers receive copies of law enforcement reports that contain so little information or indications of authenticity as to cause them to be unable to verify that a genuine law enforcement agency issued the report or accepted the filing, or if they determine that the report was fraudulent in any material aspect, they may reject the document as not being a copy of an official, valid law enforcement report.[45] Finally, because not all police report forms contain an express notice regarding criminal penalties for false statements, the Commission considers that excluding a law enforcement report on such a basis would add unnecessary consumer confusion and hardship to the process of obtaining a law enforcement report.

Some commenters were concerned that the Commission's proposal to allow consumer reporting agencies and information furnishers to make reasonable requests for additional information or documentation for an ''identity theft report'' may result in consumer confusion by requiring victims to submit different information or documentation to different companies.[46] Commenters also argued that permitting a reasonable request for additional information or documentation created the potential for abuse,[47] and could make recovery more difficult as well as delay the provision of services.[48] Permitting a reasonable request for additional information or documentation may result in victims having to submit different information or documentation to different companies. However, the requirement that the request must be reasonable should limit requests. On balance, the Commission believes that allowing consumer reporting agencies and information furnishers to make reasonable requests on a case-by-case basis will help prevent abuse of the credit reporting system and maintain the viability of the recovery process for bona fide victims as contemplated by the Act.

Other comments raised the concern that the Commission's five business day time limit on the request for additional information or documentation did not provide a long enough time period to evaluate the need for and to make an initial request.[49] The Commission

[43] *See* 18 U.S.C. 1001. Although the Commission does not have criminal authority to arrest a person or to prosecute identity theft cases directly, based on its Congressional mandate under the 1998 Identity Theft Assumption and Deterrence Act, Pub. L. 105–318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. 1028), it works closely with criminal law enforcement agencies at all governmental levels to analyze the complaints in its database and refer out possible leads for investigation. Thus, complaints made to the Commission may be subject to criminal law enforcement review in much the same way as complaints made directly to federal agencies with criminal authority.

[44] *See, e.g.*, Consumer Data Industry Association #000009 (''* * * the rule should give examples of what constitutes a 'an official, valid report') and Experian Information Solutions #000012 (''An 'official, valid' report is one that on its face demonstrates that the complainant is subject to criminal penalties for any false statements in the report.'').

[45] With respect to reports filed with an automated system, a consumer reporting agency or information furnisher could expect to receive some evidence of a filing confirmation receipt along with the copy of the actual report, thereby allowing it to verify with the agency that a report was filed.

[46] See, *e.g.*, Consumers Union #EREG–000002 (''* * * 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.'').

The National Association of Attorneys General (#000008) suggested an alternative to allowing variable requests for additional information or documentation in that, ''* * * the regulations should provide one form containing all information that identity theft victims are expected to provide, such as the FTC affidavit form which is already available on the FTC's website.''

The referenced ID Theft Affidavit was developed by the Commission in coordination with consumer advocate organizations and financial institutions. While it was intended to save time for victims by giving them a uniform means to provide basic information about their identity theft claim, it never purported to cover all necessary information, and companies might ask for additional information. *See* Instructions for Completing the ID Theft Affidavit at *http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf.* Given the variety of forms of identity theft, it is doubtful that a single form could contain all information that all identity theft victims could be expected to provide, yet not be overly burdensome to complete. For example, an information furnisher may need to confirm passwords or other security measures when unauthorized account use has occurred.

[47] Consumers Union (#EREG–000002) also was concerned that requests for additional information or documentation may be abused by consumer reporting agencies and information furnishers. The Commission disagrees that it has opened the door to abusive requests. The Commission carefully crafted the proposed rule to require that requests for additional information or documentation be reasonable.

[48] Finally, Consumers Union (#EREG–000002) argued that allowing requests for additional information would delay the placement of extended fraud alerts. The Commission stated in the examples in the final rule that a law enforcement report submitted for the purpose of obtaining an extended fraud alert, even if filed using an automated system, should not trigger a request for additional information or documentation. In developing this example, it did not appear to the Commission that requests for extended fraud alerts needed to be subject to special scrutiny as there had been no evidence that fraud alerts under the voluntary placement system were requested without cause. No commenters raised any objection to this example. Thus, the Commission anticipates that victims will obtain extended fraud alerts without additional delay in accordance with the placement procedures set forth by the Act.

In any event, consumers who have not already done so may place an initial alert while their request for an extended alert is being processed. Thus, consumers who immediately place an initial fraud alert will receive all of the benefits of this alert.

[49] *See, e.g.*, Michigan Credit Union League #EREG–000024 (''We believe that the five-business day window may be insufficient time to allow credit unions to request the additional information. This might particularly impact credit unions that are very large or very small. Large credit unions could potentially be inundated with identity theft reports and not be able to request that information within the proposed time frame. Small credit unions may not have the staffing or be open more than one to two days per week. This would prevent them from being able to request this information.'') and Keycorp #EREG–000007 (''We believe it is appropriate to include additional documentation requirements in the definition of ''Identity Theft Report.'' However, we are greatly concerned with regard to the timing of the information request by the furnisher or credit reporting agency. Given the complexity of the financial transactions that may be involved in the ID theft claim, coupled with the number of Identity Theft Reports an institution may receive, we do not believe that five business days is sufficient time to receive the Identity Theft Report, evaluate the transaction information contained in the Report, determine what additional information may be required from the consumer to validate the claim, and request the information from

Continued

recognizes that five business days may not be long enough to fairly evaluate the law enforcement report for some consumer reporting agencies or information furnishers. The consequences may be to force them to choose between accepting the law enforcement report as the complete identity theft report regardless of whether the identity theft claim is legitimate, or sending out *pro forma* requests for additional information or documentation, which may or may not be reasonable under the circumstances. The former instance would undermine the Commission's reasons for allowing reasonable requests of information or documentation initially—to minimize abuse of the credit reporting system. The latter instance might result in an increase of consumer complaints and disputes regarding the reasonableness of the information or documentation requests, which would not be a beneficial use of consumers' time and resources. Thus, the Commission considers that allowing consumer reporting agencies and information furnishers to have a longer period of time to evaluate the law enforcement report will better limit fraud and provide a better outcome overall for consumers.

Commenters' suggestions on a longer time period ranged from ten to thirty days (both calendar and business days). The Commission has determined to modify its proposed rule to allow consumer reporting agencies and information furnishers to have fifteen calendar days to make an initial request for additional information or documentation. Fifteen calendar days is approximately five business days more than the Commission had originally proposed, which should allow all consumer reporting agencies and information furnishers sufficient time to determine whether additional information or documentation is needed, but should not cause victims undue delay.

Some commenters also requested an opportunity to make further requests for information or documentation, if necessary.[50] The Commission believes that an exchange of communication between consumer reporting agencies or information furnishers and consumers will allow for a more thorough investigation of the validity of identity theft claims. Furthermore, some consumers may make mistakes in what information or documentation they provide initially and would benefit from further opportunities to furnish the correct information.

Commenters generally suggested one time period to cover both initial and multiple requests or made no specific suggestions. The Commission believes that additional requests should be permitted. However, one time period for both initial and multiple requests could result in the first request of additional information or documentation being made on the last day of the time period, with subsequent requests being made at indefinite times thereafter. The Commission believes that this could unfairly delay the recovery of victims. Therefore, the Commission has determined to retain a limited time period (fifteen calendar days) for an initial request to ensure that an investigation commences promptly, and to set a time limit of fifteen additional days after the initial request for any further requests for information or documentation, as well as a final determination on acceptance or rejection of the ''identity theft report.'' However, in the event that a consumer should submit the additional information or documentation too late in this second fifteen day period for a consumer reporting agency or an information furnisher reasonably to be able to review it, the Commission will allow the consumer reporting agency or information furnisher an additional five days to make a final determination on acceptance or rejection of the ''identity theft report.'' For example, if the additional information or documentation is received on day fourteen of this second fifteen day period, the consumer reporting agency or information furnisher may have five days, if needed, to make a final determination on acceptance or rejection of the ''identity theft report.''

Thus, although in many instances it should take much less time to reach a final determination,[51] under no circumstances will it take longer than thirty-five days.[52] This timing balances the needs of victims to have a finite process for submitting an identity theft report, with the needs of consumer reporting agencies and information furnishers to verify the identity theft. To ensure that victims will understand the operation of this final rule and to facilitate their ability to obtain an identity theft report with minimal delay, the Commission will conduct consumer and business education to advise victims of their rights. The Commission anticipates that should consumer reporting agencies and information furnishers make requests for additional information or documentation, they will inform consumers about the time frame within which information or documentation should be submitted and the outcome if the requested information or documentation is not submitted in a timely manner.

Additionally, a number of commenters requested that the Commission develop a procedure by which consumer reporting agencies or information furnishers could reject identity theft reports. The Commission believes that consumer reporting agencies and information furnishers already have a procedure for rejecting identity theft reports. If the document or documents the consumer presents do not meet the definition set forth in the final rule, the consumer reporting agencies and information furnishers can reject them.

A number of commenters also requested that the Commission clarify the clause ''filed by the consumer'' in paragraph (2) to mean filed directly by the consumer, and not by someone else on behalf of the consumer, as a means of preventing illegal credit repair.[53] The

---

the consumer. We believe a minimum of fifteen business days is required to properly evaluate and react to an Identity Theft Report responsibly.'').

[50] *See, e.g.*, American Bankers Association #EREG–000034 (''* * * the Commission should permit more than a single request. In many cases, it will be necessary to request additional information in order to properly handle the claim as it progresses.'').

[51] The Commission expects that consumer reporting agencies and information furnishers will make any requests as expeditiously as possible. In particular, it expects that any supplemental requests for information or documentation would be made as soon as practicable to allow consumers sufficient time to respond. It further notes that in practice, many victims may make initial contact with a company by a telephone call as opposed to submission of a law enforcement report. At that time, many consumer reporting agencies or information furnishers likely would discuss with the victim what information or documentation, if any, in addition to the law enforcement report may be needed to validate the identity theft claim so that victims can expedite the process by submitting all necessary documentation together. Thus, the Commission anticipates that a consumer reporting agency or information furnisher may develop an even more efficient and accommodating process for assisting identity theft victims than the minimum standard for timing set forth under this final rule.

[52] While not directly on point, the Commission observes that the section 611 time period for reinvestigation of disputed information can range from thirty to forty-five days depending on whether the consumer provides the consumer reporting agency with additional relevant documentation. 15 U.S.C. 1681i. The maximum thirty-five day period here is adequate because, unlike under section 611, the procedures here explicitly contemplate a dialogue, if needed, within the second fifteen day period, with a possible additional five days for final review.

[53] *See, e.g.*, Consumer Bankers Association #000007 (''We believe an important corollary to the requirement that the identity theft report be filed with an appropriate law enforcement agency is that the report must be filed by the consumer, and not by another entity. CBA is concerned that credit repair clinics and other unscrupulous individuals should not be permitted to file identity theft reports on consumers' behalf.'').

Commission believes that there may be a number of legitimate reasons why a third party (*e.g.*, a guardian or an attorney-in-fact) might file an identity theft report on behalf of a consumer. The Commission believes that to the extent a third party is filing false identity theft reports on behalf of a consumer, the Commission has provided consumer reporting agencies and information furnishers with sufficient flexibility within the definition to determine the validity of the identity theft report just as if the consumers had filed the false identity theft reports themselves. In fact, to the extent a consumer reporting agency or information furnisher recognizes the same filer or a pattern to the filings, it could consider such information as a factor in determining the validity of the identity theft report.

In the NPRM, the Commission provided examples of when it would or would not be reasonable to request additional information or documentation. Commenters asked for clarification on these examples. With respect to the first example,[54] a number of commenters wanted to be able to request additional information or documentation even if the victim provided a suitable police report. Some commenters pointed to section 609(e) of the FCRA, which allows a business to ask for a police report and an affidavit to verify a claim of identity theft before providing copies of the victim's identity theft related transaction records, as an example that Congress intended that they should be able to request additional information or documentation in all cases.[55]

The Commission views the examples as sufficiently clear; they convey that it is reasonable for a consumer reporting agency or information furnisher to request additional information or documentation if the in-person police report is lacking in necessary information or the consumer reporting agency or information furnisher can identify some other reasonable concern underlying the request. Thus, although the examples are intended to demonstrate that victims should not be required to provide redundant information for no discernable reason, they make equally clear that consumer reporting agencies or information furnishers are not prevented from taking reasonable steps to verify the identity theft.

Moreover, Congress did not include the requirements of section 609(e) in the definition of ''identity theft report.'' Instead, it granted the Commission rulemaking authority to determine how the ''identity theft report'' should most appropriately be defined. The Commission believes that it would be overly burdensome to consumers if consumer reporting agencies and information furnishers could request additional information or documentation without an underlying rationale. Further, as discussed above, the Commission believes that it has provided consumer reporting agencies and information furnishers with sufficient flexibility to verify identity theft claims.

Some commenters were concerned that specific language in the first example, that ''the report was fraudulently obtained,'' excluded reports that were counterfeit or otherwise falsified.[56] For the sake of clarity, the Commission has changed this language to ''the report was fraudulent.'' At least one commenter noted that the fifth example seemed unclear.[57] The Commission agrees and considers that the caution against unreasonable redundancy in example 5 is already covered by the other examples. Therefore, it has deleted the fifth example. The remaining examples are unchanged.

C. Section 613.1: Duration of Active Duty Alerts

Under section 112 of the Act, service members who meet the definition of an active duty military consumer[58] are permitted to place an active duty alert in their consumer report maintained by a nationwide consumer reporting agency covered under the definition of section 603(p) of the FCRA. The Act sets a minimum period of 12 months for the duration of the active duty alert, but required the Commission to determine if this period should be longer. In the NPRM, the Commission proposed to maintain the duration of the active duty alert at 12 months because it believed that 12 months would cover adequately the time period for which the majority of service members would be deployed. A number of commenters, including the one service branch commenting directly on the issue, supported the Commission's proposal.[59]

Opposing commenters generally suggested that service members should be able to choose their own duration or select among options of pre-determined lengths.[60] The Commission has

[54] Example 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. 69 FR 23378.

[55] *See, e.g.*, Consumer Data Industry Association #000009 (''In addition, the verification element is consistent with the FACT Act provisions, codified in FCRA section 609(e), with respect to the obligations of a business entity to disclose information to an identity theft victim. Those provisions give the entity the discretion always to request the following from the victim, in order to verify the claim of identity theft: (i) A copy of a police report evidencing the claim; and (ii) a properly completed (I) copy of a standardized affidavit of identity theft developed and made available by the Commission; or (II) an affidavit of fact that is acceptable to the business entity for that purpose. [Footnote 12: FCRA 609(e)(2)(B); 15 U.S.C. 1681g(e)(2)(B) (emphasis added).] However, as discussed below, CDIA is concerned that the illustrative examples in the Proposed Rule appear to suggest that in some instances, it would be unreasonable for a consumer reporting agency to request a fraud affidavit or similar information when the consumer provides a police report. Such a suggestion would create unjustified inconsistency, because the FCRA itself permits furnishers to use their discretion to request such information in similar circumstances.'').

[56] *See, e.g.*, Consumer Data Industry Association #000009 (''Although the example would permit requests for additional information if there is some indication that the report was obtained fraudulently, the example should also permit additional information if the report was fraudulently created or altered.'').

[57] *See, e.g.*, Consumer Data Industry Association #000009 (''(5) If the information the information furnishers or the consumer reporting agencies are seeking is already found in the law enforcement report which is otherwise satisfactory, it would not be reasonable to request that the consumer fill out the same information on a different form. The point of this example is unclear.'').

[58] FACT Act sec. 111, *codified at* FCRA sec. 603(q)(1), 15 U.S.C. 1681a(q)(1).

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 01(a)(13) of Title 10 U.S.C.; and

(B) Is assigned to service away from the usual duty station of the consumer.

The Commission notes that the United States Marine Corps (#000004) requested clarification of this definition due to concerns that reservists do not have a usual duty station and that some service assignments may only be temporary. However, with respect to active duty alerts, Congress charged the Commission solely with considering whether to lengthen the duration of the active duty alert.

[59] *See, e.g.*, Office of the Judge Advocate General, Department of the Navy #000011 (''The active duty alert should remain at 12 months. * * * The disadvantage of a longer duration for the active duty alert is that service members may need to remove the alert instead of allowing it to expire. For understandable security reasons it will be more difficult to remove an alert than it is to place one. Delays experienced in removing an alert can negatively impact an individual's ability to establish lines of credit or procure loans. Additionally, a 12-month duration for an alert strikes the balance of meeting the active duty military member's needs without being an undue burden on consumers or creditors.'').

[60] *See, e.g.*, Navy Federal Credit Union #000022 (''While many tours of active duty may span 12

Continued

understood that a term of deployment is generally 12 months or less. Deployments may be extended, but service members will not know if their deployments will be extended before they leave on their initial deployment. Thus, it would seem, in the majority of cases, that it would be impossible for service members to accurately select a duration greater than 12 months.

The Commission considers that a better solution would be for service members whose deployments are greater than 12 months to place a subsequent active duty alert.[61] In the NPRM, the Commission asked for comments on the ability of service members to do so, particularly if they already are deployed. The Commission received only a few responsive comments.[62] The one comment on the issue from a military service branch indicated that its personnel likely would have access to email, regular U.S. mail and/or a commercial phone line at least during a portion of the deployment. The Commission expects that the active duty alert may be renewed by using at least some of these communication methods.[63]

Accordingly, the Commission adopts the duration of the active duty alert without modification.

D. Section 614.1: 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. The Commission proposed that the 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 Commission also proposed examples of the kind of information that it might be reasonable to request to match consumers with their files as well as for additional identification. In developing this proposal, the Commission determined that the central consideration was the balance between 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. Because the Commission considered that the risk of harm may differ depending on a variety of factors including the service being requested,[64] it sought to develop a standard of proof that had sufficient flexibility to accommodate these differences. Moreover, the Commission viewed the consumer reporting agencies as being in the best position to assess these differences. Commenters were generally supportive of the Commission's approach,[65] but many requested clarifications on various points.

A few commenters requested clarification that the Commission's rule did not require that a consumer reporting agency be able to match consumer-provided information with their file information to a perfect degree.[66] This rule is not intended to reach the question of whether a consumer reporting agency should match information completely, but rather to set forth the type of information that would allow the agency to accurately find the right consumer's file in its database, and as necessary, determine that the requester is in fact the consumer.

Other commenters were concerned that the rule not be used to make it more difficult for consumers to obtain the requested services.[67] Because the rule states that consumer reporting agencies ''shall develop and implement

months, many do not. We believe that the agency should prescribe flexibility for those cases where a servicemember's deployment extends beyond the 12-month duration and broaden the definition of 'active duty alert.' We suggest that the rule be written to allow a servicemember to place an alert from 12 to 24 months or, in the alternative, allow the servicemember to place an alert for the expected term of his or her tour of duty.'').

[61] The Commission notes that although the Act is silent on the placement of subsequent alerts, it would be illogical to read the Act otherwise because service members may go on deployments that meet the elements of the definition of the term ''active duty military consumer'' several times during their service careers.

[62] *See, e.g.*, Office of the Judge Advocate General, Department of the Navy #000011 (''Navy personnel on extended deployments will in most circumstances have access to Email, regular U.S. Mail and/or a commercial phone line at least during a portion of the deployment. Assuming one of these methods of communication will be sufficient to establish or extend an active duty alert then it should not be difficult for a service member to accomplish. Additionally, deploying units frequently hold pre-deployment briefings at which deploying personnel can be briefed on the active duty alert and the option of identifying a personal representative capable of extending the active duty alert if it becomes necessary.''); Michigan Credit Union League #EREG–000024 (''If necessary, we don't believe that it would be difficult to extend an active duty alert, since part of the process of being called to active duty often requires a service person to designate a person as their power of attorney. If the active duty is going to be extended, then the service person or a designated power of attorney could request an extension.''); and Consumers Union #EREG–000002 (''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.'').

[63] Communication also should be made easier for deployed service members because they only need to contact one of the consumer reporting agencies when placing an active duty alert. Under section 605A of the FCRA, the contacted consumer reporting agency must refer the request for placement to the other nationwide consumer reporting agencies. 15 U.S.C. 1681c–1.

[64] For example, given the function of fraud alerts in preventing identity theft, they need to be placed without delay, yet they seem unlikely to be placed by someone other than the consumer or without authorization from the consumer. Thus, unless these circumstances were to change, it would not seem necessary to require more identification than is needed to match the consumer's file. With respect to requests for removal of fraud alerts, however, there would seem to be some incentive for someone other than the consumer, such as an identity thief, to remove them. A delay due to greater scrutiny of the requester would likely cause less harm than an improper removal, and would thus justify greater proof of identity. 69 FR 23374.

[65] *See, e.g.*, Consumer Bankers Association #000007 (''The Proposed Rule requires consumer reporting agencies to 'develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity.' We commend the FTC for determining that the consumer reporting agencies are in the best position to determine what should suffice as 'appropriate proof of identity' in these circumstances. Like the FTC, we believe that the consumer reporting agencies are best equipped to evaluate the risks of misidentifying the consumer as well as the types of information that would be necessary to identify the consumer properly. Therefore, we urge the FTC retain this approach in the Final Rule.'').

[66] *See, e.g.*, Sprint Corporation #EREG–000013 (''The Commission should make clear that when a file match process is used, it is not requiring that there be a 'full match.' For example, a consumer may provide his address as 143rd. yet other records may identify the address as 143rd Street or Terrace. Similar variances or even keystroke errors can occur with street numbers and customer names. If a 100 percent match were required, a high percentage of requests would likely be rejected by automated systems and fall out for manual processing, which would entail length delays and add significant costs. The Commission should make clear that it is not requiring reporting agencies and information furnishers to use, build or modify systems requiring a 100 percent match with no variance allowed, if they use a file match process.'').

[67] *See, e.g.*, Consumers Union #EREG–000002 (''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.'').

reasonable requirements for what information consumers shall provide,'' the Commission believes that this required element of reasonableness, taken together with the examples of types of reasonable information, will limit the likelihood that a consumer reporting agency would make identification unduly difficult for consumers.

Commenters also were concerned about the reasonableness of allowing consumers to be asked to provide their full Social Security numbers.[68] The Commission believes it is reasonable for consumer reporting agencies to request the full Social Security number if they determine it to be necessary. Consumer reporting agencies already have the full number so the risk that accompanies a new disclosure is minimal. Furthermore, because names, addresses, and birth dates are not always unique to a consumer, full Social Security numbers may be necessary to ensure that consumer reporting agencies match the consumer with the correct file. Moreover, the use of partial Social Security numbers may not provide sufficient accuracy when an agency is working with a large database.

Some commenters were concerned that differing standards of identification would lead to confusion [69] or delays in service.[70] Under the voluntary systems of fraud alert placement and fraudulent information blocking existing prior to the Act, the Commission saw no evidence of consumer confusion in the standards of identification different consumer reporting agencies selected. One standard could also lead to consumers being asked for too much information in order that every consumer reporting agency satisfy the standard of the one consumer reporting agency that needed the most information due to its particular circumstances.

One commenter requested clarification of ''current methods of authentication'' in paragraph (b)(2).[71] The Commission used the term ''current'' to demonstrate that authentication methods may change over time and the examples should be sufficiently flexible to adapt accordingly. However, to avoid confusion, the Commission has deleted the word ''current.''

Some commenters requested that additional types of information be added to the examples.[72] It was not the Commission's intention to specify every form of authentication that a consumer reporting agency could use. Rather, the intent was to distinguish the type of information that might be sufficient for finding consumers' files from the type of information that could prove that the consumers are who they purport to be. Therefore, the Commission does not deem it necessary to include additional authentication methods. However, in paragraph (b)(1), the Commission has added the language ''current and/or recent'' before ''full address'' to make clear that consumer reporting agencies may request additional addresses for consumers who have recently relocated as it may be less apparent that such information may be necessary to find a consumer's file.

Except for the changes to the examples referenced above, the Commission makes no changes to the rule or the examples.

III. Final Regulatory Flexibility Analysis

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 (*i.e.*, in general, those with less than $6,000,000 in average annual receipts). 5 U.S.C. 603–605.

The Commission hereby certifies that the final rules will not have a significant economic impact on a substantial number of small entities. The final rules apply to consumer reporting agencies, including agencies that are small entities, if any; persons that furnish information to consumer reporting agencies (''information furnishers''), including persons that are small entities, if any; and to users of consumer reports who are seeking to extend credit to consumers, including users that are small entities, if any. The Commission has concluded that currently there are no nationwide consumer reporting agencies that are small entities (with less than $6 million in average annual receipts). In the NPRM, the Commission stated that a precise estimate of the number of small entities that are other consumer reporting agencies (with less than $6 million in average annual receipts) and users of consumer reports within the meaning of the proposed rules was not currently feasible. In the NPRM, therefore, the Commission asked several questions related to the existence, number and nature of small business entities covered by the proposed rules, as well as the economic impact of the proposed rules on such entities. The Commission received no comments responsive to these questions. Thus, the Commission has been unable to determine precisely how many, if any, consumer reporting agencies, information furnishers, and users of consumer reports are small entities within the meaning of the final rules. Based on its own experience and knowledge of industry practices and members, however, the Commission believes that although there may be a number of small entities among the other consumer reporting agencies,

[68] *See, e.g.*, Consumers Union #EREG–000002 (''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.'').

[69] *See, e.g.*, Equifax Information Systems #000023 (''Allowing adjustments commensurate with the risk of harm allows too much leeway and could result in different standards and risk evaluations by nationwide consumer reporting agencies and data furnishers. One data furnisher or nationwide consumer reporting agency may accept the proof of identity and the others not, resulting in confusion to consumers and the system.'').

[70] *See, e.g.*, Consumers Union #EREG–000002 (''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 Act requires nationwide consumer reporting agencies to refer fraud alerts to each other for placement in a consumer's report. The Commission does not believe that it is necessary for the final rule to determine how these consumer reporting agencies comply with this requirement of the Act. The Commission considers that the final rule provides these consumer reporting agencies with the necessary flexibility to comply, and expects that they will select the correct standard of identification to ensure their compliance, or modify the standard as necessary should they be found to be out of compliance.

[71] Consumer Data Industry Association #000009 (''It is unclear what is meant by 'current' methods.'').

[72] *See, e.g.*, Consumer Data Industry Association #000009 (''CDIA also suggests that the final rule include as examples of alternative proof of identity copies of pay stubs and W–2 forms.'') and TransUnion LLC #000018 (''* * * we ask that a consumer's previous address (if the consumer has resided at the present address for less than two years) be an example of appropriate information.'').

information furnishers and the users of consumer reports, and the economic impact of the final rules on a particular small entity could be significant, overall the final rules likely will not have a significant economic impact on a substantial number of small entities. The Commission believes further that the regulations will have a minimal impact on small entities because the regulations give these entities flexibility to adapt their existing requirements to ensure that they are providing correctly the services requested by consumers.

Accordingly, this document serves as notice to the Small Business Administration of the agency's certification of no effect. Nonetheless, the Commission has determined to publish a Final Regulatory Flexibility Analysis with the final rules. Therefore, the Commission has prepared the following analysis:

A. Need for and Objectives of the Rule

The Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108–159, 117 Stat. 1952 (FACT Act or the Act), directs the Commission to adopt rules 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. In this action, the Commission promulgates final rules to fulfill the statutory mandate. The rules are authorized by and based upon sections 111 and 112 of the FACT Act.

B. Significant Issues Raised by Public Comment

The Commission received no public comments on the specific impact, if any, of the rules on small entities. As explained above, the Commission has been unable to determine precisely how many, if any, consumer reporting agencies, information users, and users of consumer reports are small entities within the meaning of the final rules. Overall, however, the Commission believes that the final rules likely will not have a significant economic impact on a substantial number of small entities. Furthermore, as discussed below, the Commission has determined that with respect to small entities, if any, the final rules do not include a collection of information requirement subject to the Paperwork Reduction Act of 1995.

The Commission, however, has considered that § 603.3 of the rules, which defines the term ''identity theft report'' and establishes that it may include additional information or documentation to help information furnishers or consumer reporting agencies determine the validity of the alleged identity theft, could apply to small entities, if any. As proposed in the NPRM, the request, if any, for additional information would have to have been made no later than five business days after the date of receipt of the report or the request by the consumer for a particular service, whichever came later. A few commenters questioned certain aspects of the process for requesting additional information set forth in § 603.3, and they directly commented on the potential impact of the process on small entities, if any. For example, the commenters stated that a small business may need more than five business days to request additional information from a consumer, especially in light of the potential increase in the number of identity theft reports that will be received by small businesses, which may have limited staffing and hours of operation. Specifically, the commenters indicated that a small business may need more than five business days to receive an identity theft report, process it, review its contents, and search its files to determine whether it needs additional information from a consumer.[73] In this Statement of Basis and Purpose, the Commission has explained its consideration of and response to those comments. The Commission has made certain changes in § 603.3 of the final rules that should further minimize its impact on all information furnishers and consumer reporting agencies, which would include those, if any, that may be small entities. These changes, which provide information furnishers or consumer reporting agencies with additional opportunities, over a longer period of time than originally proposed (30 days), to request more information from consumers, are explained above in the discussion of the revisions made to § 603.3 of the rules.

C. Small Entities to Which the Rules Will Apply

As described above, the final rules apply to consumer reporting agencies, including agencies that are small entities, if any; information users, including agencies that are small entities, if any; and to users of consumer reports, including users that are small entities, if any. In the NPRM, the Commission stated that 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 was not currently feasible. The Commission, however, invited comment and information on this issue. No comments addressed this issue, and no information with respect to small entities that might be affected by the rules was provided. Thus, based on the lack of response to its request for comments, the Commission has been unable to determine precisely how many, if any, consumer reporting agencies, information furnishers and users of consumer reports are small entities within the meaning of the final rules.[74]

D. Projected Reporting, Recordkeeping and Other Compliance Requirements

In the NPRM, the Commission tentatively determined that with respect to small entities, if any, the proposed rules did not include a collection of information subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501; 5 CFR 1320). The rules do contain collections of information affecting individual consumers and those activities have been separately approved under the Act, as described in section IV, *infra.* The Commission, however, sought comment on any paperwork burden that the proposed rules may impose on small entities to ensure that no burden had been overlooked. No comments addressed this issue. Accordingly, the Commission has determined that with respect to small entities, if any, the final rules do not include a collection of information subject to the Paperwork Reduction Act of 1995.

The Commission recognizes, however, that consumer reporting agencies, information furnishers and users of consumer reports, including those that might be small entities, if any, may incur some indirect, incidental expenses associated with the regulatory scheme established by the rules. Most of these expenses will be in the form of printing,

[73] *See, e.g.,* Coalition to Implement the Fact Act #000019, the Michigan Credit Union League #EREG–000024, America's Community Bankers #000024, and the Juniper Bank #000026.

[74] In addition, to the extent the rules may indirectly affect small governmental jurisdictions (*e.g.,* local police departments that may provide reports about identity theft to consumers), which are defined as small entities pursuant to the RFA (5 U.S.C. 601(5)), the U.S. Census Bureau's *Governments Integrated Directory* as enumerated for the 2002 Census of Governments, suggests there are approximately 85,000 such jurisdictions nationwide. It is not feasible, however, for the Commission to estimate precisely how many, if any, of these jurisdictions may provide reports about identity theft to consumers.

copying, mailing and filing costs associated with processing and reviewing identity theft reports, validating the information received from consumers, and requesting additional information from consumers, if necessary, to determine the validity of the alleged identity theft or the consumer's proof of identity. It is not feasible for the Commission to estimate precisely such expenses without information regarding the volume of the aforementioned activities. It is likely, however, that some of the aforementioned expenses would be incurred anyway in the ordinary course of business.

E. Steps Taken To Minimize Significant Economic Impact of the Rules on Small Entities

The Commission invited 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.

The Commission received no information or suggestions in response to these questions. As explained above, however, the Commission has written the final rules, and made certain changes to the final rules, to minimize their impact on all entities that are subject to the rules, including small entities, if any, that may be subject to the rules. For example, the Commission has written the final rules to provide information furnishers or consumer reporting agencies with additional opportunities, over a longer period of time than originally proposed (30 days), to request more information from consumers.

IV. Final Paperwork Reduction Act Analysis

In accordance with the Paperwork Reduction Act, as amended, 44 U.S.C. 3501 *et seq.*, the Commission submitted the proposed rules to the Office of Management and Budget (''OMB'') for review. The OMB has approved the rules' information collection requirements through June 30, 2007, and has assigned OMB control number 3084–0129. The Commission did not receive any comments relating to its original burden estimates for the rules' information collection requirements.

V. Final Rules

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

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

■ Accordingly, for the reasons set forth in the preamble, the Commission amends title 16 of the Code of Federal Regulations as follows:

■ 1. Add part 603 to read as follows:

PART 603—DEFINITIONS

Sec.

Authority: Pub. L. 108–159, sec 111; 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 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 person, 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:

(i) Makes such request not later than fifteen 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;

(ii) Makes any supplemental requests for information or documentation and final determination on the acceptance of the identity theft report within another fifteen days after its initial request for information or documentation; and

(iii) Shall have five days to make a final determination on the acceptance of the identity theft report, in the event that the consumer reporting agency or information furnisher receives any such additional information or documentation on the eleventh day or later within the fifteen day period set forth in paragraph (a)(3)(ii) of this section.

(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 fraudulent, 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.

■ 2. Add Part 613 to read as follows:

PART 613—DURATION OF ACTIVE DUTY ALERTS

Sec.

613.1 Duration of active duty alerts.

Authority: Pub. L. 108–159, sec. 112(a); 15 U.S.C. 1681c–1.

§ 613.1 Duration of active duty alerts.

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

■ 3. Add Part 614 to read as follows:

PART 614—APPROPRIATE PROOF OF IDENTITY

Sec.

614.1 Appropriate proof of identity.

Authority: Pub. L. 108–159, sec. 112(b).

§ 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, current and/or recent 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 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.

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 04–24589 Filed 11–2–04; 8:45 am]

BILLING CODE 6750–01–P

DEPARTMENT OF STATE

22 CFR Part 171

[Public Notice 4841]

RIN 1400–AB85

Availability of Information to the Public

AGENCY: State Department.

ACTION: Final rule.

SUMMARY: This rule makes final the Department's proposed rule published on March 31, 2004. The rule revises the Department's regulations governing access by the public to information that is under the control of the Department in order to reflect changes in the provisions of basic underlying laws and executive orders pertaining to access to information (*i.e.*, the Freedom of Information Act, the Privacy Act, Executive Order 12958 on National Security Information, the Ethics in Government Act) and in the Department's procedures since the last revision of the Department's regulations on this subject. The Department received one non-substantive comment, and proposes no changes to the proposed rule. The proposed rule is therefore issued as final.

EFFECTIVE DATE: This rule is effective on November 3, 2004.

ADDRESSES: Persons wishing to make requests for information under these regulations should address such requests to: Margaret P. Grafeld, Director, Office of Information Programs and Services, U.S. Department of State, SA–2, 515 22nd St., NW., Washington, DC 20522–6001. Tel: 202–261–8300; FAX: 202–261–8590.

Persons with access to the Internet may also view this notice by going to the regulations.gov Web site at *http://www.regulations.gov/index.cfm.*

FOR FURTHER INFORMATION CONTACT: Margaret P. Grafeld, Director, Office of Information Programs and Services, U.S. Department of State, SA–2, 515 22nd St., NW., Washington, DC 20522–6001. Tel: 202–261–8300; FAX: 202–261–8590.

SUPPLEMENTARY INFORMATION: The Department's proposed rule was published as Public Notice 4653 at 69 FR 16841–16853 on March 31, 2004, with a 90-day public comment period. The Department received one non-substantive comment regarding Reading Room hours of operation, which was satisfied by the availability of the Department's FOIA Web site 24 hours a day. Additionally, while the Department does not accept FOIA requests via e-mail, we are beginning to accept requests via our Web site.

The Freedom of Information Act (FOIA), the Privacy Act (PA), and certain portions of the Ethics in Government Act and Executive Order 12958, as amended, provide for access by the public to records of executive branch agencies, subject to certain restrictions and exemptions. 22 CFR part 171 sets forth the Department's regulations implementing the access provisions of those statutes and the Executive Order. Since the last publication of the regulations in the 1980's, there have been significant changes in the law governing access to government information by the public, particularly with respect to the FOIA and the Executive Order. In addition, certain court decisions have been rendered that affect such access provisions.

A major revision of the Freedom of Information Act was enacted in 1996, the so-called Electronic Freedom of Information Act. The changes effected by the Electronic Freedom of Information Act amendments of 1996 included provisions with respect to the form in which agencies are required to