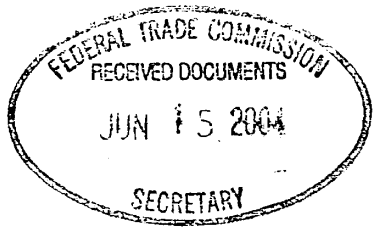
RUSSELL W. SCHRADER
Senior Vice President
Assistant General Counsel



VISA

June 15, 2004

By Hand Delivery

Federal Trade Commission
Office of the Secretary
Room H-159 (Annex J)
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Re: FACTA Identity Theft Rule, Matter No. R411011

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa U.S.A. Inc. in response to the notice of proposed rulemaking ("Proposed Rule") and request for public comment by the Federal Trade Commission ("FTC"), published in the Federal Register on April 28, 2004. Pursuant to the Fair Credit Reporting Act ("FCRA"), as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), the Proposed Rule would: (1) define the terms "identity theft" and "identity theft report;" (2) determine the appropriate duration of an active duty alert; and (3) define what constitutes "appropriate proof of identity" for the purposes of placing or removing fraud or active duty alerts, blocking fraudulent trade lines or obtaining from a consumer reporting agency ("CRA") a file disclosure containing a truncated social security number. Visa appreciates the opportunity to comment on these important topics.

The Visa Payment System, of which Visa U.S.A.[1] is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud, for the benefit of its member financial institutions and their hundreds of millions of cardholders.

DEFINITION OF "IDENTITY THEFT"

The Proposed Rule would provide further definition to the term "identity theft," as defined in section 603(q)(3) of the FCRA. Specifically, the Proposed Rule would define

[1] Visa U.S.A. is a membership organization comprised of U.S. financial institutions licensed to use the Visa service marks in connection with payment systems.

VISA U.S.A. INC.
Post Office Box 194607
San Francisco, CA 94119-4607
U.S.A.
Phone 415 932 2178
Fax 415 932 2525

"identity theft" as "a fraud committed or attempted using the identifying information of another person without lawful authority."[2] In addition, the Proposed Rule would define "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual."[3]

The FACT Act amended the FCRA, in part, to assist consumers and financial institutions in combating identity theft. To this end, the FACT Act added several provisions to the FCRA that are designed to prevent the occurrences of, and to mitigate the effects of, identity theft. As a result, the definition of "identity theft" is critical in determining the scope of the conduct that entities must take steps to prevent, and in determining who may take advantage of the rights conferred on victims of identity theft.[4] For example, the definition of "identity theft" triggers provisions of the FCRA that authorize consumers to file fraud alerts, to block fraudulent trade lines and to prevent furnishers of consumer report information ("furnishers") from furnishing information that is identified as resulting from identity theft.

Definition of "Identity Theft" is Too Broad

Visa believes that the proposed definition of "identity theft" is too broad. This definition would appear to cover all types of fraudulent conduct involving credit cards, including traditional credit card fraud. While all types of identity theft involve fraud, not all types of fraud constitute identity theft. There is no basis in the language or legislative history of the FACT Act to conclude that Congress intended the term "identity theft" to cover traditional credit card fraud. If Congress intended such broad coverage, the unique term "identity theft" would be unnecessary and, instead, Congress could have used a more general term to describe the scope of the fraud. The proposed definition of "identity theft" significantly would go beyond instances in which an identity thief uses another person's personal information to establish an account in that person's name or to take over the person's account, such as by using personal information to change the address on an account and to receive replacement credit cards at that address. This is the core conduct that the FCRA identity theft provisions are intended to address. Defining "identity theft" broadly to include traditional types of credit card fraud would impose significant costs on financial institutions and would dilute the effectiveness of remedies for identity theft victims, such as fraud alerts.

The Proposed Rule would define the term "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual."[5] This definition also lists information that would qualify as "identifying

---

[2] 69 Fed. Reg. 23,370, 23,377 (Apr. 28, 2004).
[3] *Id.*
[4] The Supplementary Information to the Proposed Rule ("Supplementary Information") seems to imply that the Proposed Rule's definition of "identity theft" will apply to all uses of this term in the FCRA. However, section 603(q), which includes the FCRA definition of "identity theft" and the rulewriting authorization, is entitled "Definitions relating to fraud alerts." As a result, the authority of the FTC to define the term "identity theft" as used throughout the FCRA is unclear.
[5] 69 Fed. Reg. at 23,377.

information," including name, social security number, driver's license number and fingerprint, all of which are traditional means used for identification. In fact, the Proposed Rule's definition of "identifying information" is taken from a definition of "means of identification" found in a criminal provision of the U.S. Code concerning the fraudulent use of identification documents.[6]

Nevertheless, Visa is concerned that, like the reference to "attempted" fraud discussed below, this broad definition of "identifying information" could unnecessarily broaden the scope of identity theft. This definition determines the information that must be used in connection with a fraud in order for that fraud to qualify as identity theft for the purposes of the FCRA. For example, the proposed definition of "identifying information" appears to transform instances of traditional credit card fraud, such as an individual purchasing goods or services with a stolen credit card number, into identity theft because a fraud would have been committed using another person's identifying card number. Visa believes that a credit card is only a method of payment and not a means of identification or proof of age.

If a credit card number was considered "identifying information," the definition of identity theft would go significantly beyond instances in which an identity thief uses another person's personal information to establish an account in that person's name. Including traditional credit card fraud in the definition of "identity theft" may significantly increase claims of identity theft, fraud alerts and requests to block information as to individual transactions, rather than entire tradelines, which are already covered by the dispute provisions of the Truth in Lending Act ("TILA"). In addition, these processes are costly to CRAs, as well as to users of credit reports, and further proliferation of fraud alerts can only dilute their effect on users of credit reports and the actions that they take in response to these alerts.

Although traditional credit card fraud can be harmful to consumers, TILA provides sufficient remedies for victims of this fraud and obviates the need to address this conduct under the FCRA. TILA and Regulation Z provide that, for open-end credit plans, a consumer may dispute an extension of credit and other specified types of transactions that appear on the consumer's periodic statement.[7] Once a consumer asserts a billing error, a creditor must investigate and resolve the dispute within the time period provided for under Regulation Z. Specifically, consumers may dispute various types of billing errors, which include "[a] reflection on . . . a periodic statement of an extension of credit that is not made to the consumer" and "[a] reflection on . . . a periodic statement of an extension of credit for property or services not accepted by the consumer."[8] Until the creditor resolves the billing error, a consumer may withhold payment of the disputed amount and the creditor is prohibited from attempting to collect the disputed amount or making an adverse report to any person about the consumer's credit standing or about a delinquency relating to this amount because the consumer failed to pay the disputed amount.[9] In addition, a cardholder's liability for unauthorized transactions is

---

[6] *See* 18 U.S.C. § 1028(d)(7).
[7] The TILA billing error provisions are found in 15 U.S.C. § 1666. The Regulation Z billing error provisions are found in 12 C.F.R. § 226.13.
[8] 12 C.F.R. §§ 226.13(a)(1), (3).
[9] 12 C.F.R. §§ 226.13(d)(1)-(2).

limited to the lesser of $50 or the amount charged on the account before a card is reported as lost or stolen. Under these provisions, the vast majority of frauds involving an existing credit card account are resolved promptly with no adverse effect to the consumer's credit history. Further, these frauds typically do not exhibit the repetitive patterns associated with true identity theft, and the steps that financial institutions take to prevent these frauds are different.

Visa believes that expanding the definition of "identity theft" to include traditional credit card fraud is not necessary in order to mitigate the effects of this fraud on consumers. For the reasons discussed above, Visa strongly urges the FTC to limit the definition of "identity theft."

Attempted Fraud as "Identity Theft"

Visa is concerned that including "attempted" fraud within the definition of "identity theft" would expand significantly the scope of conduct that entities must take steps to prevent, and would increase greatly the number of consumers authorized to take advantage of the rights that the FCRA confers upon victims of identity theft. Visa believes that the additional costs of expanding the concept of identity theft beyond the traditional notion of an individual opening an account in another person's name or taking over another person's account will outweigh the benefits. If a fraud is attempted but not completed, the system will have worked successfully to avert identity theft and the consumer will have suffered little, if any, harm. Any harm that the consumer will have suffered from the attempt can be, or already will have been, adequately addressed. Visa strongly urges the FTC to limit the definition of "identity theft," and specifically to exclude fraud that is attempted but not successfully completed.

The Supplementary Information provides two examples suggesting why the definition of identity theft should be expanded to include attempted fraud. First, the Supplementary Information points out that a consumer's credit score may be lowered if an inquiry for the consumer's credit report is made as a result of an unsuccessful attempt by an identity thief to open an account in the consumer's name.[10] The Supplementary Information notes that this "victim" should be entitled, presumably pursuant to section 605B of the FCRA, to have this fraudulent trade line removed from his or her credit report file. However, this possibility is already addressed under the existing FCRA. More specifically, if a consumer becomes aware that a credit report inquiry was made as a result of an attempted fraud, the consumer can dispute the accuracy of this inquiry with a CRA, pursuant to existing section 611 of the FCRA. Section 611(a)(1)(A) would require the CRA to conduct a reinvestigation of the accuracy of this information or simply delete it. If the reinvestigation revealed that the information was inaccurate, incomplete or could not be verified, the CRA would be required to delete the disputed information from the consumer's file.[11] In addition, upon receipt of the dispute, the CRA would be required to inform the furnisher of that information of the dispute, and the furnisher would then bear similar duties as the CRA.[12] As a result, a fraudulent inquiry on a

[10] 69 Fed. Reg. at 23,371.
[11] FCRA §§ 611(a)(1)(A), 611(a)(5)(A).
[12] FCRA § 623(b)(1).

consumer's credit report file already can be removed without any modification to the term "identity theft" and without the adverse consequences that will follow from an expansion of this term.

Second, the Supplementary Information indicates that a consumer who has learned of an attempted fraud may wish to place an initial fraud alert on his or her credit report file.[13] However, the requirements for an initial fraud alert are sufficiently broad to allow the consumer to obtain such an alert without requiring a modification of the definition of "identity theft" to include attempted fraud. To place an initial fraud alert, a consumer must only be able to assert a good faith "suspicion that the consumer . . . is about to become a victim of fraud."[14] The FCRA does not require the consumer to be certain that he or she will become a victim of fraud, but only requires the consumer to be able to assert in good faith a "suspicion." A consumer who is aware of an attempted fraud using his or her identifying information clearly would be able to assert in good faith a suspicion that he or she is about to become a victim of identity theft and, as a result, place an initial fraud alert on his or her credit report file.

Use of Identifying Information "Without Lawful Authority"

Visa supports the FTC's determination that the definition of "identity theft" should include the limitation that the identifying information be used "without lawful authority."[15] If an individual permits another to use his or her identifying information to commit a fraud, the individual who granted the permission to use the information in a fraudulent manner should not be entitled the recourse intended for legitimate victims of identity theft by the FCRA.

DEFINITION OF "IDENTITY THEFT REPORT"

The FCRA requires a consumer to provide an identity theft report in order to obtain an extended fraud alert, to block fraudulent trade lines or to prevent furnishers from furnishing information that resulted from identity theft. Section 603(q)(4) of the FCRA directs the FTC to define the term "identity theft report." Section 603(q)(4), however, requires that the term, at a minimum, must mean a report "that alleges an identity theft," "is a copy of an official, valid report filed by a consumer with an appropriate Federal, State, or local law enforcement agency" and "the filing of which [would subject] the person filing the report to criminal penalties" if the person included false information in the report. The Proposed Rule would elaborate on this definition by requiring the report to allege the identity theft "with as much specificity as the consumer can provide" and may require the report to include information or documentation that a furnisher or a CRA may "reasonably" request for the purpose of determining the validity of the alleged identity theft.[16]

---

[13] 69 Fed. Reg. at 23,371.
[14] FCRA § 605A(a)(1).
[15] 69 Fed. Reg. at 23,377.
[16] *Id.* at 23,377-23,378.

The requirement that a consumer provide an identity theft report before obtaining an extended fraud alert, blocking a fraudulent trade line or preventing a furnisher from furnishing information that resulted from identity theft, functions as a safeguard against the misuse of these powerful tools. In the Supplementary Information, the FTC accurately points out that a consumer could file a report with a law enforcement agency in an automated manner that does not involve interaction with any law enforcement officer and that includes only a simple allegation of identity theft.[17] The consumer's unilateral ability to create an identity theft report in this manner raises the specter that consumers may create and use identity theft reports inappropriately.[18] The Proposed Rule attempts to address these concerns, without disadvantaging bona fide victims of identity theft, by requiring that the consumer allege the identity theft with as much specificity as possible and by permitting furnishers and CRAs to request additional information from the consumer.[19] Visa strongly supports the goal of the FTC to balance the needs of victims of identity theft against the risk of misuse of the powerful tools conferred upon victims of identity theft.

Nevertheless, Visa believes that the final rule should provide additional guidance concerning the ability of furnishers and CRAs to request additional information. Although the Proposed Rule provides illustrative examples of when it may or may not be reasonable to request additional information, significant uncertainty remains. For instance, it is not clear whether a furnisher or a CRA must request additional information if the furnisher or the CRA determines that the initial report provided by the consumer is inadequate. Although the Supplementary Information indicates that the ability to request additional information "is intended to compensate for a report which does not rise to the level of the ideal law enforcement report," the Supplementary Information does not state that a furnisher or a CRA must take steps to compensate for an inadequate report.[20] In addition, the consequences of the answer, or the lack of an answer, to a request for additional information are not addressed in the Proposed Rule. If a consumer does not respond to a request for additional information or provides a wholly inadequate response, it is not clear whether the furnisher or the CRA must renew its request for additional information, or inform the consumer that without additional information the furnisher or the CRA cannot honor the consumer's request. Furthermore, if a furnisher determines that the law enforcement report provided by the consumer does not qualify as an identity theft report, it is unclear whether the furnisher or the CRA must communicate this decision to the consumer, and if so, how this determination should be communicated. Visa believes that a CRA or a furnisher should not be required to act on an identity theft report if it reasonably requests additional information or documentation and that information or documentation is not provided or is

---

[17] *Id.* at 23,372.

[18] In addition, because reports could be completed and filed with no physical or direct contact with a law enforcement officer, a "so-called" credit repair clinic, armed with only the consumer's personal information, could fraudulently file a report in the consumer's name in order to later use such a report to block accurate, but negative, information. Unlike legitimate credit counseling services, "so-called" credit repair clinics often attempt to remove accurate, but negative, information from consumer's credit files by overwhelming CRAs with disputes concerning the accuracy of credit files.

[19] 69 Fed. Reg. at 23,377.

[20] *Id.* at 23,372.

inadequate to determine the validity of the alleged identity theft, and that the furnisher's or CRA's only obligation is to inform the consumer of this fact.

Visa also believes that the FTC should clarify that an identity theft report must be based on a report filed with a law enforcement agency that has statutory arrest authority. The Supplementary Information seems to indicate that any agency that has civil or criminal law enforcement authority would qualify as an "appropriate" law enforcement agency.[21] However, the Supplementary Information recognizes that the "identity theft report" "could provide a powerful tool for misuse, allowing persons to engage in illegal activities in an effort to remove or block accurate, but negative information in their consumer reports."[22] Although the Proposed Rule would require an identity theft report to be based upon a report "the filing of which [would subject] the person filing the report to criminal penalties" if the person included false information in the report, this may not be sufficient to deter individuals determined to clear accurate but negative credit history through fraudulent means.[23] Visa believes that the arrest authority of a law enforcement agency would act as an important safeguard and deterrent against the fraudulent use of the remedies designed to assist victims of identity theft.

In addition, Visa believes that the FTC should clarify that an identity theft report can only result from a report filed by a consumer. The minimum FCRA requirements for the definition of "identity theft report" and the Proposed Rule's definition of "identity theft report" both state that an identity theft report is a copy of report "filed by a consumer."[24] Neither indicates that an identity theft report can be a copy of a report filed by a consumer's personal representative or agent. The FTC should state specifically in the final rule that a report filed by a "so-called" credit repair clinic will never qualify as an identity theft report.

DURATION OF ACTIVE DUTY ALERT

Section 605A(c) of the FCRA requires a nationwide CRA, upon direct request by an active duty military consumer and after receipt of appropriate proof of the consumer's identity, to include an active duty alert in his or her credit report file for "a period of not less than 12 months, or such longer period as the [FTC] shall determine, by regulation." The Proposed Rule would establish the duration of the active duty alert at 12 months.[25]

Visa supports the FTC's determination that the active duty alert should not exceed 12 months. The Proposed Rule would strike the appropriate balance by protecting the majority of active duty military consumers for the duration of their deployments. If the duration of active duty alerts exceeded the duration of most deployments, military consumers could be inconvenienced when seeking to obtain credit after returning to their usual duty stations. Visa

---

[21] *See id.* n.9 (noting that a complaint filed with the FTC Identity Theft Data Clearinghouse would qualify as an "identity theft report" in part because it is filed with the FTC, which is a "federal law enforcement agency").
[22] *Id.* at 23,372.
[23] *Id.* at 23,377-23,378.
[24] FCRA § 603(q)(4)(B); 69 Fed. Reg. at 23,377.
[25] 69 Fed. Reg. at 23,378.

suggests that the FTC reiterate in the final rule that if an active duty alert does not sufficiently cover the length of a military consumer's deployment, the military consumer may place another active duty alert upon expiration of the first alert.

DEFINITION OF WHAT CONSTITUTES "APPROPRIATE PROOF OF IDENTITY"

The FCRA requires a CRA to obtain appropriate proof of a consumer's identity before placing a fraud or active duty alert on the consumer's credit report file, before blocking fraudulent trade lines and before truncating the consumer's social security number in a credit file disclosure. Section 112(b) of the FACT Act directs the FTC to define what constitutes "appropriate proof of identity" for these purposes. The Proposed Rule would require CRAs to "develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity."[26] In addition, the Proposed Rule would require CRAs in developing these requirements to "[e]nsure that the information is sufficient to enable the [CRA] to match consumers with their files" and also to "adjust the information to be commensurate with an identifiable risk of harm arising from misidentifying the consumer."[27]

Visa strongly supports the FTC's determination that a CRA must develop and implement reasonable requirements for what information constitutes proof of identity. A "reasonable requirements" standard will provide each CRA with the flexibility to develop and implement requirements that are uniquely tailored to the CRA's operations. Moreover, allowing a CRA to develop its own "reasonable requirements" will allow the CRA to minimize disruptions to existing business practices and procedures, except where necessary to do so.

Although the Proposed Rule provides examples of information that may constitute reasonable information requirements for proof of identity, the Proposed Rule does not address the identification process itself. The FCRA requires a consumer to make a request to block a fraudulent trade line or to receive a truncated credit file disclosure; however, the "consumer, or an individual acting on behalf of or as a personal representative" of the consumer may request a fraud or active duty alert.[28] Visa believes that the final rule should make it clear that information that is not provided by the consumer, or in the case of fraud or active duty alerts, by an individual acting on behalf of, or as a personal representative of, the consumer, would not constitute appropriate proof of identity. Visa also believes that the final rule should make it clear that a "so-called" credit repair clinic can never qualify as a consumer's agent or personal representative in the case of fraud alerts.

---

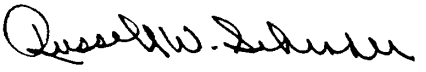
[26] 69 Fed. Reg. at 23,378.

[27] *Id.*

[28] FCRA §§ 605A(a)(1), 605A(b)(1), 605(A)(c); FCRA § 605B(a) (stating that a CRA must block a trade line in a consumer's credit report file "that the consumer identifies as information that resulted from an alleged identity theft"); FCRA § 609(a)(1) (stating that a CRA must truncate a credit file disclosure "if the consumer to whom the file relates requests" such truncation).

Visa appreciates the opportunity to comment on these important topics. If you have any questions concerning these comments, or if we may otherwise be of assistance in connection with this matter, please do not hesitate to contact me, at (415) 932-2178.

Sincerely,



Russell W. Schrader
Senior Vice President and
Assistant General Counsel