VISA

September 15, 2006

By Electronic Delivery

Russell W. Schrader
Senior Vice President
Assistant General Counsel

Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
Attention: Docket No. R-1255

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Attention: Comments
RIN 3064-AD00

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, DC 20580
Attention: The Red Flags Rule,
Project No. R611019

Mary F. Rupp
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428

Office of the Comptroller of the Currency
250 E Street, SW
Mail Stop 1-5
Washington, DC 20219
Attention: Docket No. 06-07

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 2006-19

Re: Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003

Ladies and Gentlemen:

This letter is submitted on behalf of Visa U.S.A. Inc. in response to the proposed regulations ("Proposal") by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (collectively, the "Agencies"), published in the Federal Register on July 18, 2006.[1] The Proposal requests public comment on rules requiring the implementation of reasonable policies and procedures to detect "Red Flags" indicating the possible existence of identity theft and assessing change-of-address requests (collectively, "Red Flag Rules") and rules requiring reasonable policies and procedures to respond to a notice of an address discrepancy ("Address Rule"), under sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"). Visa appreciates the opportunity to comment on this important matter.

[1] Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 71 Fed. Reg. 40,786 (July 18, 2006).

Visa U.S.A. Inc.
P.O. Box 194607
San Francisco, CA 94119-4607
U.S.A.

t 415 932 2178
f 415 932 2525

The Visa Payment System, of which Visa U.S.A.[2] 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. In calendar year 2005, Visa U.S.A. card purchases exceeded a trillion dollars, with over 510 million Visa cards in circulation. 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 Visa's member financial institutions and their hundreds of millions of cardholders.

THE RED FLAG RULES SHOULD BE HARMONIZED WITH EXISTING REQUIREMENTS

Visa is pleased that the Agencies have taken a risk-based approach to the Red Flag Rules; however, Visa is concerned that, contrary to the Agencies' apparent intent, the Red Flag Rules could be interpreted to require complex and sophisticated new programs to combat identity theft. Visa believes that such programs are unnecessary because financial institutions already have in place extensive and effective programs that address identity theft. In most cases, financial institutions should be able to meet the purposes of the Red Flag Rules by documenting existing procedures and making relatively simple modifications to existing procedures. Accordingly, Visa believes the Agencies should harmonize the Red Flag Rules with the existing requirements and procedures for verifying the identity of customers and protecting customers from fraud involving their accounts.

One of the greatest risks to consumers due to identity theft arises from the account-opening process. It is unauthorized accounts that give rise to the need for consumers to correct, sometimes repeatedly, their credit histories. Conversely, the largest losses to financial institutions arise from fraud on existing accounts where common law, federal legislation, and industry standards, including Visa's "zero liability" policy, protect consumers from liability for fraudulent transactions. In both cases, well-developed programs are already in place to address these risks. Visa believes that the final Red Flag Rules should allow financial institutions to develop their own risk-based procedures regarding identity theft that consider their own experiences, as well as the protections already afforded by section 326 of the USA PATRIOT Act for opening accounts, and the Truth in Lending Act, the Electronic Fund Transfer Act, and the Uniform Commercial Code for fraud on existing accounts.

The Red Flag Rules Should Give Financial Institutions Broad Discretion to Implement a Risk-Based Identity Theft Prevention Program

Section 114 of the FACT Act directs the Agencies to adopt guidelines that are not inconsistent with the policies and procedures required under the Customer Identification Program rules prescribed under section 326 of the USA PATRIOT Act ("CIP Rules").[3] The CIP Rules are designed to address concerns for national security and, in connection with the war against trafficking in illegal drugs, the prevention of money laundering. Section 114 of the FACT Act contemplates that the procedures adopted by financial institutions to meet the

---

[2] 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.

[3] 31 U.S.C. § 5318(*l*); 31 C.F.R. § 103.121.

requirements of the CIP Rules also would address the risk of the opening of fraudulent accounts to commit identity theft. In fact, this is the case, and a properly implemented customer identification program ("CIP") should also satisfy the account-opening requirements of the Red Flag Rules. However, as proposed, the Red Flag Rules could be read to require substantial modifications to the systems that financial institutions have developed to identify and verify the identity of each customer and, therefore, would be inconsistent with the policies and procedures currently used in accordance with the CIP Rules.

As noted in the Proposal,[4] the Agencies should adopt Red Flag guidelines that are consistent with the CIP Rules. Despite the clear mandate set forth in section 114 of the FACT Act, the Red Flag Rules, as proposed, could be viewed as requiring substantial modifications to the systems that financial institutions have developed to identify and verify each customer at the time an account is opened and, therefore, would be inconsistent with the CIP Rules. Visa believes that, consistent with the plain language of section 114, the Agencies should modify the requirements relating to account-opening processes to provide that satisfaction of the CIP Rules also satisfies the Red Flag Rules in connection with opening accounts.

Specifically, section __.90(d)(2)(i) of the Red Flag Rules would require a financial institution to include in its Identity Theft Prevention Program ("Program") "reasonable policies and procedures designed to prevent and mitigate identity theft in connection with the opening of an account," including policies and procedures to "[o]btain identifying information about, and verify the identity of, a person opening an account." This general requirement is consistent with the CIP Rules. However, the proposed Red Flag Rules could be read to impose additional and substantial obligations on financial institutions to detect, prevent, and mitigate identity theft in connection with the opening of an account, namely to:

(1) "Detect the Red Flags identified pursuant to paragraph (d)(1) of this section;"[5]

(2) "Assess whether the Red Flags detected pursuant to paragraph (d)(2)(ii) of this section evidence a risk of identity theft;"[6] and

(3) "Address the risk of identity theft, commensurate with the degree of risk posed,"[7] such as by taking one or more of nine listed actions, some of which appear to be wholly unrelated to the context of account-opening processes.[8]

Visa believes that each of these additional measures is inconsistent with the CIP Rules, which, as the Proposal correctly states, only "require verification of the identity of customers opening accounts."[9] Although some or all of these measures may be part of an

---

[4] 71 Fed. Reg. at 40,792.
[5] Proposal § __.90(d)(2)(ii).
[6] In addition to this general requirement, the Agencies have proposed that "[a]n institution or creditor must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft." Proposal § __.90(d)(2)(iii). For ease of reference and consistency with the Proposal, references to the proposed regulations use the shared numerical suffix of each of the agency's regulations. 71 Fed. Reg. at 40,789.
[7] Proposal § __.90(d)(2)(iv).
[8] Proposal § __.90(d)(2)(iv)(A)-(I).
[9] 71 Fed. Reg. at 40,792.

existing CIP adopted by a financial institution, the final Red Flag Rules should make it clear that the requirements of the rules for account openings can be met by an appropriate CIP.

Similarly, for existing accounts, financial institutions have a wide variety of programs in place to address fraud conducted on these existing accounts. The federal Truth in Lending Act, the Electronic Fund Transfer Act, and the Uniform Commercial Code, as well as state common law, limit the extent to which losses for fraudulent transactions on existing accounts can be imposed on consumers. Indeed, financial institutions have gone beyond these requirements to protect their customers from losses due to fraud, such as through Visa's implementation of its "zero liability" policy. Because they absorb the losses from fraudulent transactions, financial institutions have well-developed programs that have withstood years of supervisory scrutiny to control these risks. Moreover, financial institutions are continually updating their programs to combat account fraud. These programs range from judgmental reviews of individual transactions to sophisticated neural networks, such as those employed by Visa and its members, that are designed to identify patterns of fraudulent activity. While the various components of these programs may not be cataloged and described in one place today, the Red Flag Rules should focus on documenting this process to control fraud losses, rather than creating new and different, and less cost-effective, programs based on a list of possible fraud indicators.

In this regard, Visa is concerned that the list of Red Flags in the Red Flag Rules may be viewed as a presumptive list that applies to all accounts at all financial institutions so that financial institutions must incorporate the Red Flag Rules on the list into their own programs or justify why they did not. While Visa believes that the list is helpful to financial institutions, particularly smaller financial institutions, because it might alert them to certain issues or practices about which they were unaware, Visa believes that specific incorporation of Red Flags from the list should be at the discretion of each financial institution. Each financial institution should only be required to document how its procedures address the risks of account fraud. Visa believes that the Agencies should avoid adopting a rule that would lead to "checklist" methods of examining financial institutions for compliance, whereby examiners could criticize an institution's policies and procedures for neglecting to identify and address each and every Red Flag, including those that are unrealistic or unforeseen. Visa urges the Agencies to expressly state in the text of the Red Flag Rules that a financial institution may implement a Program that identifies, assesses, or responds to those particular Red Flags as indicated by the institution's own risk evaluation. Correspondingly, the Red Flag Rules should expressly provide that an institution complies with the Red Flag Rules even if its Program does not include specific policies or procedures to identify, assess, or respond to any individual Red Flag prescribed by the Agencies.

Clarify Ability to Use "Other Means" to Assess Change-of-Address Requests

Section __.91 of the Red Flag Rules requires a card issuer to assess the validity of a change of address if the card issuer receives a change-of-address notice and, within a short period afterwards, receives a request for an additional or a replacement card for the account. The concern is that an identity thief may have sent in the change-of-address request, unbeknownst to the cardholder, and then have a new card sent to the fraudulent address. In these cases, verifying the authenticity of either the changed address or the request for the new

card should prevent the fraud. As a practical matter, verification is likely to be achieved by verifying the identity of the person making the request. Section __.91(c)(3) of the Red Flag Rules would allow a financial institution that is a "card issuer" to assess the validity of a change-of-address request by a cardholder by notifying the cardholder or by using "other means," "in accordance with the policies and procedures the card issuer has established pursuant to [the Red Flag Rules]." As the Proposal recognizes,[10] the requirements of this provision are specified by section 114 of the FACT Act. Visa believes that the Agencies should permit each card issuer to implement its own risk-based policies and procedures that allow the issuer to assess the validity of a change-of-address request through authentication of the person making the request and other means that are in accordance with the issuer's Program. Accordingly, Visa believes that it is important for the Agencies to retain this provision in the final rules. In addition, Visa believes that this provision should be modified to clarify that card issuers are permitted to apply appropriate systems used to authenticate customers to protect against fraud to satisfy this requirement of the Red Flag Rules.

THE ADDRESS RULE SHOULD CONFORM TO THE STATUTE

Section 315 of the FACT Act requires the Agencies to prescribe "reasonable policies and procedures" applicable to a user of a consumer report "to reconcile the address of the consumer with the consumer reporting agency [("CRA")] by furnishing such address to such [CRA] as part of information regularly furnished by the user for the period in which the relationship is established."[11] The statute contemplates a simple system for updating a consumer's address at a CRA by having a user of consumer reports that also furnishes information to the CRA report the different, presumably new, address to the CRA. This process will enhance the accuracy of address information maintained in the files of consumer reporting agencies from which consumer reports are produced, even though it cannot be counted on to definitively establish a consumer's address, if only because some consumers legitimately use different addresses for different purposes.

The Agencies have proposed to require a user of consumer reports to independently confirm the accuracy of a consumer's address—"[e]ven when the user is able to form a reasonable belief that it knows the identity of the consumer."[12] Specifically, the Address Rule would require, in relevant part, a user to "develop and implement reasonable policies and procedures for furnishing an address for the consumer *that the user has reasonably confirmed is accurate* to the [CRA] from whom it received the notice of address discrepancy."[13] There is no basis in the language or structure of section 315 of the FACT Act to require a user of a consumer report to confirm the accuracy of the address itself. The Agencies should strike this additional requirement from the final Address Rule. Placing this confirmation duty on furnishers of information to CRAs is not only inconsistent with the statute, it also is inconsistent with the voluntary scheme of furnishing information to CRAs that is a cornerstone of the Fair Credit Reporting Act ("FCRA").

---

[10] 71 Fed. Reg. at 40,794.
[11] 15 U.S.C. § 1681c(h)(2).
[12] 71 Fed. Reg. at 40,796.
[13] Proposal § __.82(d)(1) (emphasis added).

The FCRA reflects a longstanding policy of voluntary reporting to CRAs. The FACT Act amendments did not modify that policy. Financial institutions have strong incentives to maintain accurate information about their customers as a fundamental part of conducting their businesses and have established policies and procedures to comply with a wide range of regulatory requirements that enhance their ability to maintain and furnish accurate information about their customers. The Address Rule, as proposed, would impose new requirements on financial institutions that voluntarily furnish information to CRAs in accordance with the FCRA.

In order to maintain and promote broad participation in the consumer reporting system, the Agencies should adhere to the language set forth in section 315 of the FACT Act and require a user to reconcile the address information solely "by furnishing such address to such [CRA] as part of information regularly furnished by the user for the period in which the relationship is established."[14] Thus, if the user "[c]an form a reasonable belief that it knows the identity of the consumer for whom the consumer report was obtained," pursuant to section __.82(d)(1)(i), the user should be allowed to comply with its obligation to "reconcile" the consumer's address with the CRA solely by furnishing to the CRA the address information maintained by the user "as part of information regularly furnished by the user for the period in which the relationship is established."[15] Permitting a user to furnish the consumer's address as part of the information regularly furnished by the user is consistent with the statutory language and the purposes of section 315 because, in this particular context, the user also should establish or maintain a "continuing relationship" with the consumer, as described in section __.82(d)(2)(ii). Moreover, by incorporating the statutory language in the final rule, the Agencies would promote the implementation of policies and procedures that are consistent with the existing voluntary reporting policy under the FCRA.

ADDITIONAL ISSUES

The Red Flag Rules Should Not Require Approval by the Board of Directors

As noted above, the issues covered by the Red Flag Rules are already being addressed by financial institutions. The Proposal seeks comment on whether the provision of the Red Flag Rules regarding oversight "properly allocates the responsibility for oversight and implementation of the Program between the board and senior management."[16] Visa believes that, in light of these existing programs, establishing formalistic approval requirements going forward is unnecessary. Although each financial institution should be required to assign oversight responsibilities for the development, implementation, and maintenance of its Program, the Red Flag Rules should not mandate specific duties and assign these duties to the board and to senior management. To do so will divert the attention of senior management and the board of directors from other issues of greater significance to the safety and soundness of the financial institution. Instead, the Agencies should adopt final rules that grant discretion to each financial institution to adopt general oversight responsibilities for its Program and permit

[14] 15 U.S.C. § 1681c(h)(2)(B)(ii).
[15] *Id.*
[16] 71 Fed. Reg. at 40,793.

the institution to assign the particular oversight responsibilities that are consistent with the institution's risk evaluation.

The Agencies' Comment on the Equal Credit Opportunity Act Should Be Retracted

In a footnote, the Agencies state that, in the event that a creditor receives a consumer report containing a fraud alert or an active duty alert, "a creditor must take reasonable steps to verify the identity of the individual in accordance with the requirements of [section 605A of the FCRA] before extending credit, closing an account, or otherwise limiting the availability of credit."[17] In this context, the Agencies proffer a comment on the application of the Equal Credit Opportunity Act ("ECOA") to these situations. This footnote raises complex issues under the ECOA and FCRA that require a more thorough airing than this footnote. Therefore, the footnote should be retracted in the final rules.

* * * *

We appreciate the opportunity to comment on this important matter. 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

[17] *Id.* at 40,792 n.23.