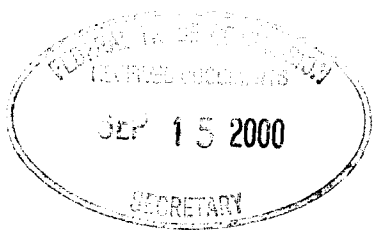
RUSSEL W. SCHRADER
Senior Vice President and
Assistant General Counsel



VISA

September 15, 2000

By Hand Delivery and Electronic Delivery

Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Identity Theft Victim Assistance Workshop

Dear Sir:

This comment letter is submitted on behalf of Visa U.S.A. Inc. ("Visa") in response to the request for comment issued by the Federal Trade Commission ("FTC") on issues relating to ways in which the industry, law enforcement and the government can assist victims of identity theft. Visa also applauds the FTC's plans to hold a workshop on these issues on October 23, 2000 ("Workshop"). We appreciate the opportunity to comment on this important matter.

The Visa Payment System, of which Visa U.S.A. is a part, is the largest consumer payment system in the United States and in the world, with more volume than all other major payment cards combined. Visa is part of a worldwide association of over 21,000 financial institution members ("Members") that individually offer Visa-brand payment services. In fact, Visa now has over one billion cards circulating worldwide. These Visa-branded cards are held by consumers around the globe, and generate over $1.6 trillion in annual volume worldwide and over $700 billion per year in the U.S. At peak volume, Visa's system processes nearly 4,000 card-related transactions per second. In 1999, the Visa network processed 11 billion credit card transactions worldwide.

Preventing Fraud Resulting From Identity Theft

Visa has been a leader in combating fraud -- including identity theft -- for more than a decade. To guard against unauthorized access to information in the Visa system, we have long employed the most advanced security procedures, protections and technology available. The following are just a few of the tools that Visa and its Members have used to detect and prevent identity theft-related fraud.

Application Verification System

Visa and its Members participate in an application verification system that verifies an applicant's address, telephone and Social Security number and

VISA U.S.A. INC.
Post Office Box 8999
San Francisco, CA 94128-8999
U.S.A.
Phone 650 432 3111
Fax 650 432 2145

whether the address, telephone and/or Social Security number utilized on submitted applications have previously appeared on fraudulent applications or prior credit card fraud transactions.

Card Activation

Most Visa bankcard issuers ("Issuer") use a card activation method under which the Issuer waits for the customer to confirm that a card has been received by him or her before activating the account. Under this method, cards are blocked from use at the time of mailing. For the card to be activated, the cardholder typically must call the Issuer, often from the same phone number previously provided to the Issuer by the cardholder, and must confirm receipt and provide proof of identity.

Materials to Issuers on Identity Theft Fraud

Visa, along with other bankcard associations, has helped develop a video and other materials on identity theft that are designed to help Issuers combat fraud related to identity theft.

Data Security Requirements

Visa was the first card company in the industry to develop and publish data security requirements for any entity holding card data (such as merchants, gateways, internet service providers, etc.). This program includes education for merchants, merchant self-evaluations and logical firewall testing (the latter is in the pilot stage now). With these requirements in place, the theft of information that can facilitate identity theft is reduced.

These extensive fraud detection and prevention programs have achieved significant success. For instance, the ratio of fraud-to-sales on Visa cards stood at 0.15% in 1992. Last year, it was down to a record-breaking rate of just 6 cents per $100, or 0.06%. Indeed, during recent years the absolute number of fraudulent transactions in the Visa system has actually been reduced, even as Visa card volume has soared. We are extremely proud of the success of our many fraud prevention efforts.

However, Visa recognizes that credit and debit card fraud and theft will never be eliminated completely, and that instances of identity theft generally are clearly on the rise. Those who specialize in defrauding consumers and financial institutions are extremely sophisticated; they constantly employ new mechanisms and technologies to circumvent existing protections and stay one step ahead of detection. Thus, recognizing that fraud does occur, Visa and its Members have chosen voluntarily not to hold their customers liable for unauthorized use of their Visa payment cards. More specifically, in April 2000, a new Visa operating regulation went into effect that creates a "zero liability" policy that virtually eliminates consumer liability in cases of unauthorized use of Visa payment cards. This "zero liability" policy covers the use of all Visa consumer card products -- including debit and credit cards. Thus, a consumer will not be held liable for unauthorized use of Visa payment cards -- including fraud resulting from identity theft.

Assisting Identity Theft Victims

Visa and its Members recognize that identity theft victims often face the daunting task of preventing further misuse of their identifying information and correcting damage done to their credit histories by identity thieves. In this regard, it is important to note that both consumers *and* financial institutions are victims when a consumer's identity is stolen. Consumers often are protected by law from liability for many losses that result from fraud -- including identity theft -- and, as indicated above, Visa has adopted a "zero liability" policy for the unauthorized use of Visa payment cards. Thus, it is often the financial institution that incurs the monetary losses from identity theft and other types of fraud. As a result, financial institutions have a strong interest -- from both a risk perspective and from a customer-service perspective -- to help their customers in combating identity theft in the first instance and in helping their customers in preventing further misuse of their identifying information once identity theft has occurred. As a result, financial institutions may undertake a number of steps to assist their customers who are victims of identity theft. For example, some financial institutions establish a central number to receive identity theft questions, and may share fraud alerts that they receive across their various lines of business. In addition, many financial institutions have undertaken efforts to educate their customers on the steps to take if they should become a victim of identity theft, including advice on: the importance of contacting financial institutions and credit card issuers immediately regarding possible identity theft; the importance of filing a police report; and how to contact the three major credit bureaus to obtain a credit report and to request that a "fraud alert" be placed on the customer's credit file. Visa and its Members also have worked with law enforcement officers and prosecutors to help them understand fraud types and fraud schemes involving credit card systems -- including identity theft.

Facilitation of Fraud

In the request for comment, the FTC specifically asked whether making the process of clearing one's name less burdensome on victims could in some instances facilitate fraud. It is important for the FTC to recognize that financial institutions must be very careful in handling identity theft claims, because in some instances these "alleged" claims actually are attempts by identity theft perpetrators -- engaged in "pretext" calling -- to obtain information about a consumer. To address these issues, financial institutions have focused on implementing broad employee training programs, so that the employees -- especially customer-service employees -- are better able to help "true" victims of identity theft, without inadvertently assisting perpetrators of identity theft.

"Fraud Alerts" in Credit Reports

The FTC also specifically requested comment on how the FTC can ensure that "fraud alerts" on credit reports are seen and honored by credit grantors, so as to reduce the likelihood of further harm to the victim. We would urge the FTC not to recommend any particular approach in terms of how credit grantors must use credit reports. As

discussed above, it is typically the financial institution -- and not the consumer -- that bears the financial losses resulting from identity theft-related fraud. As a result, credit grantors already have a strong economic incentive to prevent fraud from occurring, and any agency efforts regarding how credit grantors should use credit reports for fraud purposes are unnecessary.

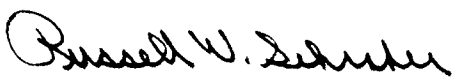
Panelist for Workshop

Visa would like to volunteer to participate as a panelist at the Workshop. In this regard, Visa attended the Identity Theft Summit that was held earlier this Spring by the Department of Treasury, in conjunction with the FTC and other agencies. At the Workshop, Visa would be happy to discuss its efforts to prevent identity theft and other types of fraud, as well as its efforts to help its Members and others better assist victims of identity theft.

* * *

Again, we appreciate the opportunity to comment on this important subject, and we look forward to working with the FTC staff on the upcoming Workshop. If we can assist you further, or if you have any questions regarding the above, please feel free to call me at 650.432.3111.

Sincerely,



Russell W. Schrader