MARK MACCARTHY
Senior Vice President
Public Policy

May 1, 2002

Federal Trade Commission
Office of the Secretary
Room 159
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
Attn: FTC File No. PO24512

Re: Consumer Information Security Workshop--Comment, PO24512

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa U.S.A. Inc. in response to the Federal Trade Commission's ("FTC") notice announcing the public workshop on consumer information security on May 20, 2002 ("Workshop"). Visa applauds the FTC's plans to hold the Workshop as a means to explore issues relating to the security of consumers' computers and the personal information stored in those computers or stored in company databases. We appreciate the opportunity to provide written comment on this important matter, and look forward to participating as a panelist in the Workshop to discuss in greater detail information security issues that affect consumers. Visa is pleased to provide comment on information security standards generally, as well as to comment on several specific questions set forth in the *Federal Register* notice announcing the Workshop.

The Visa Payment System, of which Visa U.S.A.[1] is a part, is the largest consumer payment system in the world, with more volume than all other major payment cards combined. There are more than one billion Visa-branded cards, and they are accepted at more than 24 million physical locations in more than 130 countries. Visa plays a pivotal role in advancing new payment products and technologies, including information security initiatives, to benefit its 21,000 member financial institutions and their millions of cardholders worldwide.

Visa also is the leading consumer e-commerce payment system in the world. Payment cards presently account for nearly 95 percent of online consumer transactions, and Visa card transactions account for 53 percent of that payment card portion. Moreover, we expect ten percent of Visa's overall transaction volume to come from Internet purchases by 2003, up from two percent today.

[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.
1300 Connecticut Avenue, N.W.
Suite 900
Washington, D.C. 20036
U.S.A.

General Comments on Information Security Standards

Before addressing the specific issues raised in the FTC's comment request, Visa would like to commend the FTC for the general approach taken by the FTC in its proposed security guidelines to implement Section 501 of the Gramm-Leach-Bliley Act. The approach proposed by the FTC is consistent with the approach adopted by the federal banking agencies in their final security guidelines. In particular, Visa believes that the FTC proposed approach establishes a framework that correctly focuses on the "process" that a financial institution should follow in designing and implementing an information security program, without attempting to specify in detail how a financial institution should structure its information security program or the particular safeguards to be employed in its security program. Financial institutions need flexibility in developing and implementing information security programs that best fit their particular needs in this ever-changing marketplace. As technology continues to evolve, so too will industry safeguards, including those developed by and for the nation's largest consumer payment system and its member financial institutions. Consumer confidence in e-commerce transactions is of the utmost importance, and Visa and its member financial institutions, individually and collectively, are taking significant steps to address a broad range of security-related issues.

1. The Current State of Information Security

Consumers today face a number of significant security risks -- both perceived and actual. As many businesses move operations online, the number and sophistication of threats to computer networks, servers, and consumer computers increase as well. Consumers have expressed concern that the account information they provide to merchants during online transactions might be subject to unauthorized access and use after their transactions are complete.

For example, some consumers are concerned that although their account information might be transmitted to a Web merchant in a secure fashion during a purchase or payment transaction, it will not remain secure while stored in the Web merchant's database. Media reports of intrusion by hackers into Web merchant databases have increased this concern. It should be noted, however, that the security of account information while stored in a merchant's database is not dependent on whether a consumer has conducted his or her transaction over the Internet; instead, it usually depends on the accessibility of the merchant's database through the Internet.

Moreover, in our view, consumers should continue to feel comfortable using their Visa payment cards to shop online. Visa has made great strides in addressing cardholder-not-present fraud, and in doing so hopes to overcome consumer concerns about Internet security. In fact, fraud as a percentage of Visa's total volume has declined over time, and

fraudulent use of Visa payment cards presently is at an all-time low. In the late 1980s, fraud accounted for about 0.20 percent of the total Visa card volume; in the early 1990s, it was about 0.15 percent of total card volume; and today it is a mere 0.07 percent of total card volume (or seven cents out of one hundred dollars of transaction volume).

Fraud can occur, for example, when someone uses a cardholder's account number to engage in an unauthorized transaction online. However, that credit card number may have been stolen offline and then used to purchase merchandise online. The theft of the account number might occur in a variety of ways -- for example, by breaking into a merchant's database that contains consumer account numbers, or by intercepting a consumer's credit card billing statement sent to the consumer's home. So, it is important to keep in mind that account information can be stolen offline, and then used to engage in an unauthorized transaction online.

Also, the fact that unauthorized transactions take place on the Internet does not mean that the Internet itself is a risky place for consumers to shop. If the thief has obtained a card account number, but does not actually have the card, it is only natural for the thief to use that account information in a channel of commerce, such as the Internet or mail order and telephone order, in which the card does not have to be present in order for the transaction to take place. As a result, mail order and telephone order and Internet transactions often show a higher incidence of unauthorized use. For example, as indicated above, the fraud rate for all Visa transactions is about 0.07 percent, while for card-not-present transactions it is 0.15 percent. This, of course, does not mean that it is more risky for consumers to use these channels of commerce. It simply means that those who gain unauthorized access to card information in any manner are more likely to try to use that information to engage in fraud in a card-not-present environment, such as the Internet.

It is in the interests of Visa, its members, their merchants, and consumers alike to prevent fraud. Fraud prevention protects merchants from absorbing the costs of fraud and protects consumers from the higher prices that they would have to pay in order to cover fraud losses. Fraud prevention also protects consumers from the trouble of having to exercise their rights in connection with unauthorized transactions. For these and other reasons, fraud prevention is essential to protecting the integrity of the Visa brand and maintaining the confidence of consumers and merchants that use the Visa system.

Through significant investments in technology, cooperative efforts between Visa, its members, and law enforcement agencies, and a wide variety of educational initiatives, the incidence of Visa-system fraud in recent years is at an all-time low, even as the volume of Visa card transactions has grown dramatically.

2. Security Issues Relating to Consumers' Home Information Systems

Even though Visa cardholders are already protected by Visa's zero liability policy, Visa believes that there are steps consumers can and should take to reduce their own security risks. In addition, financial institutions have a strong interest -- from both a risk perspective and from a customer-service perspective -- in helping customers secure confidential information in the first instance, and in helping customers prevent further misuse of their information once fraudulent acts, such as identity theft, have occurred. Visa currently is pursuing a number of awareness and educational initiatives, including an initiative that provides consumers with information on how to protect their cardholder information online. Visa's Web site, for example, provides an Internet Shopping Guide for consumers, with suggestions for how consumers can shop safely on the Internet, including the following:

- Shop with merchants you know and trust, and visit Better Business Bureau Online if you have questions about a particular merchant.
- Look for signs of security. Symbols like an unbroken lock or key, a URL that begins https://, or the words Secure Sockets Layer mean it is unlikely that anyone but you and the merchant can view your payment information.
- Never send payment information via e-mail. Information that travels over the Internet in an unencrypted manner (like e-mail) is not fully protected from being read by outside parties.
- Shop with reputable merchant sites that use encryption technologies that will protect your private data from being read by others as you conduct an online transaction. When you pay online, make sure that you are using a secure browser.
- Make a point of reading a merchant's privacy policy to find out what type of information is captured and how it is used.

3. Security Issues for Businesses that Maintain Consumers' Personal Information

It is critical that businesses that maintain personal information relating to consumers take appropriate steps to maintain the security of that information. Providing adequate security protection for both merchants and consumers is essential for the long-term success of e-commerce. To address consumer concerns about unauthorized access to merchant databases, Visa has developed new security requirements for cardholder data. These requirements apply to any entity holding Visa card data -- including Web merchants, gateways, and Internet service providers. These requirements prescribe how these companies should store, encrypt, and limit access to cardholder data. For example, they require Internet merchants to install firewalls, to keep security systems up-to-date, to encrypt stored data, and to use anti-virus software, among other things. These security requirements became effective May 1, 2001.

Visa also offers assistance to Internet merchants that accept Visa cards in meeting these requirements for safeguarding customer payment card data. For example, Visa provides merchants with training sessions, interactive reviews, compliance and monitoring consultation, and information on third-party firms specializing in testing and compliance.

Under this program, the top 100 e-commerce merchants -- who account for 70 percent of Internet commerce in the Visa system -- are required to have their online security procedures validated by an outside accounting or Internet security firm. Other online retailers will be subject to random security reviews by Visa. The 12 requirements of the new security program are as follows:

1. Install and maintain a working network firewall to protect data accessible via the Internet.

2. Keep security patches up-to-date.

3. Protect stored data.

4. Encrypt transmission of cardholder data and sensitive information sent across public networks.

5. Use and regularly update anti-virus software.

6. Restrict access to data by businesses' "need-to-know."

7. Assign a unique ID to each person with computer access to data.

8. Do not use vendor-supplied defaults for system passwords and other security parameters.

9. Track all user access to data by that unique ID.

10. Regularly test security systems and processes.

11. Maintain a policy that addresses information security for employees and contractors.

12. Restrict physical access to cardholder information.

In addition, in an effort to provide consumers with even greater control over when and where their card will be used, Visa recently introduced Verified by Visa, a new service that adds greater online security to credit and debit card payments. Verified by Visa enables participating card issuers to validate a cardholder's identity through the use of a password during the consumer's online checkout process while at the e-commerce merchant's site. According to a survey conducted by Visa U.S.A. last year, 70 percent of consumers indicated that they would feel safer transacting business over the Internet if they had a password to verify their identity during the course of online transactions.

4. Emerging Business Models, Technologies, and Best Practices

Visa has implemented many significant initiatives to protect the security of e-commerce transactions, including the development of new technologies to reduce the risk of unauthorized use of a cardholder's account. In fact, Visa and its member financial institutions have developed a varied arsenal of fraud control programs that helps merchants further reduce the unauthorized use of Visa payment cards. These programs are especially important in addressing Internet fraud. The programs include Verified by Visa, Address Verification, Cardholder Risk Identification, Visa's Exception File, Card Verification Value, and a pilot program for Payer Authentication.

- Verified by Visa provides an extra precaution consumers can take to prevent unauthorized use of their cards. Consumers can register for personalized passwords through the Visa member bank that issues the consumer's card or at the Visa Web site. After creating their passwords, Visa cardholders are prompted for their passwords when shopping online at participating e-commerce merchants.
- The Address Verification Service is a fraud prevention system that allows merchants to verify automatically that a shipping address provided by a cardholder at the time of purchase matches the cardholder's billing address and other information. This service helps merchants minimize the risk that

they will accept fraudulent orders from persons using stolen card account information.

- Visa's Cardholder Risk Identification Service ("CRIS") is a transaction scoring and reporting service that employs advanced neural network technologies to develop artificial intelligence risk-scoring models that help identify fraudulent transaction patterns. Issuers can use CRIS as a stand-alone fraud detection system or employ it together with their own internal fraud detection methods.
- Visa's Exception File is a worldwide database of account numbers of lost/stolen cards or other cards that issuers have designated for confiscation, referral to issuers, or other special handling. All transactions routed to Visa's processing system have their account numbers checked against the Exception File.
- The Card Verification Value ("CVV") is not printed on the card itself, but is found on the card's signature strip on the back of the card. These codes help merchants confirm that cardholders are in possession of the actual card. Online merchants and other merchants engaging in transactions where the card is not present at the time of the transaction can verify that their customers have the actual card in their possession by requesting the customer to provide the CVV from the signature strip.

* * *

Again, we appreciate the opportunity to comment on this important subject. If you have any questions concerning these comments, or if we may otherwise assist you further, please do not hesitate to contact me at (202) 296-9230.

Sincerely,

Mark MacCarthy
Senior Vice President
Public Policy