STATEMENT OF JOSHUA L. PEIREZ
SENIOR VICE PRESIDENT AND ASSISTANT GENERAL COUNSEL
MASTERCARD INTERNATIONAL INCORPORATED

BEFORE THE
HOUSE COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

"FIGHTING IDENTITY THEFT – THE ROLE OF FCRA"

JUNE 24, 2003

Good morning, Chairman Bachus, Congressman Sanders, and Members of the Subcommittee. My name is Joshua Peirez and I am Senior Vice President and Assistant General Counsel at MasterCard International in Purchase, New York. MasterCard is a global organization comprised of financial institutions throughout the world that are licensed to use the MasterCard service marks in connection with a variety of payment systems. For example, these member financial institutions issue payment cards to consumers and contract with merchants to accept such cards. MasterCard provides the networks through which the member financial institutions interact to complete payment transactions—MasterCard itself does not issue payment cards, nor does it contract with merchants to accept those cards. I thank the Subcommittee for having a hearing on this critically important issue and for giving me the opportunity to appear before you to provide information on combating identity theft.

MasterCard takes its obligations to protect MasterCard cardholders against identity theft and other forms of fraud very seriously. In fact, this issue is a top priority for MasterCard, and we have a team of experts, including many former law enforcement personnel, devoted to combating all types of fraud. We are proud of our strong record of working closely with federal, state, and local law enforcement agencies to apprehend these criminals. Included among the federal law enforcement agencies with which we work closely are the Federal Bureau of Investigation, the U.S. Secret Service, the Federal Trade Commission, the U.S. Postal Inspection Service, and others at both the federal and local level. MasterCard also fields calls from local law enforcement virtually every day. MasterCard believes its success in fighting fraud is perhaps best demonstrated by noting that our fraud rates have continuously declined over time and are at historically low levels as a percentage of transactions.

MASTERCARD CONSUMER PROTECTION AND FRAUD PREVENTION

MasterCard recognizes that identity theft and other fraudulent schemes evolve constantly, and we devote substantial resources to staying one step ahead of the criminals. We continually develop new ways to protect MasterCard cardholders and to make fraud more difficult. The following is a brief overview of just some of the efforts MasterCard has made in this area.

Issuers Clearinghouse Service

The first step in combating identity theft and other similar types of fraud is to develop techniques to prevent the crime from occurring in the first place. In our experience, accurate, reliable information is the most critical element in any identity theft prevention program. In an effort to enhance the ability of our member financial institutions to combat identity theft and other types of fraud, we require our members in the U.S. to participate in the Issuers Clearinghouse Service ("ICS"), a system built using data provided by issuers regarding, among other things, the fraudulent use of consumer data. More specifically, MasterCard's U.S. members provide ICS with data regarding customer addresses, phone numbers, and social security numbers that have been associated with fraudulent activity. MasterCard members are also required to access ICS in connection with each application to open a MasterCard account. The ICS database helps financial institutions to detect suspicious activity and prevent identity theft and other fraud before it occurs. For example, the centralized ICS database allows MasterCard members to notice whether a particular social security number was used to open a number of accounts using different addresses. Such activity may indicate that the social security number is being used for identity theft or some other fraudulent scheme. In this way, ICS provides our member financial institutions a specialized fraud prevention tool that acts as an enhancement to their other fraud prevention efforts, including those that rely on accurate, reliable consumer reports they receive under the federal Fair Credit Reporting Act ("FCRA") as discussed in greater detail below.

Payment Card Security Features

Another key part of the MasterCard fraud prevention efforts is the security features built into the payment card itself. For example, MasterCard has worked hard to make it difficult for a criminal to make use of a card number in transactions where the card is not present, such as in telephone, mail, or Internet transactions. One tool to ensure that the person presenting the number is actually the cardholder is the added security features on the card itself. MasterCard cards have the full account number printed on the card with an additional three digits on the back of the card. Many phone, mail, and Internet merchants now request these additional three digits as part of the consumer's payment transaction. In this regard, these three digits act similar to a PIN for the card and can be used to ensure that

the person presenting the card number actually has possession of the card—not just the account number.

Address Verification

Another tool to fight fraud is MasterCard's Address Verification Service ("AVS"). A criminal who obtains access to a MasterCard account number is unlikely to know both the name and the billing address of the individual who holds the account. MasterCard has developed its AVS to take advantage of this fact and prevent the criminal from using the account number. Merchants accepting a MasterCard account number by phone, mail, or Internet are increasingly using AVS as a resource and are asking for the consumer's billing address. At the time of payment, the merchant submits the billing address into the MasterCard system to verify with the card issuer that the name and billing address match the account number provided. If AVS indicates that the billing address and the account number do not match, the merchant can take additional steps to verify that the person presenting the number is the legitimate cardholder, or the merchant may simply decline the transaction.

MasterCard SecureCode

MasterCard has developed a relatively new service that allows issuers to provide added security to their cardholders when the cardholders shop on-line. A cardholder registers his or her MasterCard card with the issuer and creates a private SecureCode. Each time the cardholder makes a purchase at a participating merchant, a box will automatically pop up asking the consumer for the SecureCode—similar to the way an ATM will ask for a PIN when withdrawing money. When the cardholder correctly enters the SecureCode during an on-line purchase at a participating merchant, the cardholder confirms that he or she is the authorized cardholder. If the correct SecureCode is not entered, the purchase will not go through.

"SAFE" (System to Avoid Fraud Effectively)

MasterCard's System to Avoid Fraud Effectively ("SAFE") program is a multi-purpose tool to thwart fraud. The SAFE program is built, in part, through the use of data provided by MasterCard issuers regarding fraud-related transaction information. For example, data regarding fraudulent merchants, transactions, and other patterns of activity is incorporated in the SAFE program for use by MasterCard and its members. The SAFE program allows MasterCard to identify fraud at merchant locations and allows us to better focus our global merchant auditing programs. The SAFE program also allows us to identify potentially fraudulent actors relatively early in the process, before the problem escalates.

Site Data Protection Service

MasterCard's Site Data Protection Service ("SDP") is a multi-tiered, comprehensive set of global e-commerce/financial security services designed to help protect the web sites of its members and their on-line merchants from hack and attack. MasterCard designed SDP to be a cost-effective diagnostic tool for members and merchants to allow them to understand any systems vulnerabilities they may have. Furthermore, SDP also recommends actions that can be taken to reduce the potential systems vulnerabilities.

MasterCard's Zero Liability Protection

Recognizing that no system of protections will ever be perfect in preventing identity theft and other fraud, MasterCard has taken an important step to ensure that MasterCard cardholders are not held financially responsible when they are victimized by fraud involving U.S.-issued MasterCard accounts. We believe that our cardholder protections are the strongest available and among the most important consumer benefits a cardholder has, as these benefits provide consumers with the security and comfort necessary to make MasterCard "the best way to pay for everything that matters." A key element of our cardholder protections is our voluntary "Zero Liability" rule with respect to the unauthorized use of U.S.-issued MasterCard consumer cards. It is important to note that MasterCard's protection with respect to Zero Liability is superior to that required by law. The Truth in Lending Act imposes a $50 liability limit for the unauthorized use of a credit card. Under the Electronic Fund Transfer Act, the cardholder's liability for the unauthorized use of a debit card can be higher. MasterCard, however, provides all U.S. MasterCard consumer cardholders with even more protection. Under our rules, a cardholder victimized by unauthorized use generally will not be liable for any losses at all. This means that it is the financial institutions, and not the cardholders, that bear the financial loss when a MasterCard cardholder is victimized by identity theft or other fraud. This has greatly enhanced consumer confidence, including with respect to shopping on-line. A MasterCard cardholder can shop anywhere in the real or virtual world with the confidence that he or she will have no liability in the event that his or her account number is used without authorization.

THE IMPORTANT ROLE OF THE FCRA IN PREVENTING IDENTITY THEFT

As noted above, one of the most important tools in combating identity theft is the availability of accurate, reliable information about consumers. The role of providing this data has primarily been taken on by our nation's three major credit bureaus—Equifax, Experian, and TransUnion. These credit bureaus gather information from thousands of sources commonly referred to as "furnishers," and compile the information into individualized reports about consumers. These consumer reports contain the most accurate and reliable data available about the identities of consumers and other characteristics which are essential in combating identity theft. For example, when a bank receives an application from a consumer through the mail, the consumer report obtained from a credit bureau can be the single most important piece of information to the bank in determining whether the

individual who submitted the application is an identity thief or not. Indeed, the status of credit bureau data as useful and reliable information for identification purposes has been recognized and embodied in this nation's anti-terrorism efforts. For example, the regulation promulgated by the U.S. Treasury Department to implement Section 326 of the USA PATRIOT Act relies heavily on the use of consumer reports in properly identifying individuals who become customers of financial institutions.

The reliability of consumer report information as an identity theft prevention tool is due in great measure to the national uniform standards for credit reporting established under the FCRA. The following are some key examples of how national uniformity has ensured the quality of our credit reporting databases and has helped to combat identity theft.

Furnisher Obligations

MasterCard issuers are among the most significant suppliers of information to credit bureaus. These financial institutions report information about their accountholders regularly to the three major credit bureaus. The information generally includes the fact that an account has been established, the line of credit and current balance on the account, when the account was established, and whether the consumer has been delinquent on any payments.

Furnishers have certain obligations under the FCRA, and these obligations are the same across the country as a result of the uniform standards established by the FCRA. For example, if a furnisher determines that information it has reported to a credit bureau is not complete or accurate, the furnisher must promptly notify the bureau and provide any information necessary to make the information complete and accurate. In addition, if a consumer disputes the accuracy of information with a furnisher, the furnisher may not provide the information to the credit bureau without a notice that the accuracy is disputed. Furnishers also must reinvestigate alleged errors about information they provide to credit bureaus.

These obligations were established in 1996 in an effort to address concerns about the accuracy of information received by credit bureaus. The furnisher obligations were carefully crafted to balance between the need for furnishers to provide accurate information to credit bureaus and recognition of the fact that furnishing information to credit bureaus is completely voluntary. In particular, Congress recognized that imposing unreasonable liability or risk of litigation on furnishers could have a chilling effect on the flow of the information that is the lifeblood of the credit reporting system. As part of the delicate balance struck on this issue, and in recognition of the need for uniform information available nationwide, the FCRA precludes the states from imposing different standards.

It is important that this delicate balance be preserved. If a state were free to impose stricter liability standards on furnishers, many furnishers would be forced to re-evaluate the practice of furnishing information to credit bureaus with respect to consumers in that state. Indeed, many furnishers may have no choice but to stop furnishing information on consumers in that state rather than face the cost of litigation.

This would significantly reduce the reliability of credit bureau data. For example, card issuers and other similar financial institutions frequently have the most reliable information about a consumer's current address, change of name (*e.g.* as a result of a marriage or divorce), and other up-to-date identifying information. Stricter liability standards or more severe furnisher burdens imposed at the state level could very well curtail the availability of this information to credit bureaus and, consequently, to banks and other financial institutions that currently use it as an important identity theft prevention tool.

Contents of Consumer Reports

The contents of a consumer report are also largely standardized as a result of the national uniformity provisions of the FCRA. The FCRA establishes the time frames during which information becomes "obsolete" and can no longer be included in a consumer report. Generally, adverse items of information that are older than seven years cannot be reported in a consumer report (although the time frame expands to ten years for bankruptcy information). The FCRA preempts state laws with respect to any subject matter relating to information contained in consumer reports. This means that, as a general matter, someone's consumer report will look the same, regardless of the state in which they live. This also means that the identification information on the consumer report will be available regardless of where the consumer lives. A single standard with respect to the contents of consumer reports is critically important to ensure that the ability to properly identify customers, and therefore to provide financial products and services to them, is uniform across the country. In this regard, American consumers are extremely mobile, with millions moving from state to state in any given year. Financial institutions seeking to provide consumers with financial products or services across the country must be able to rely on a uniform standard for credit reports.

Prescreening

The FCRA governs the important underwriting and marketing tool known as "prescreening." Prescreening is a process under which a creditor may provide firm offers of credit to consumers who meet certain established underwriting criteria. Firm offers of credit often take the form of the "preapproved" offers that people receive in the mail. If an individual responds by requesting the credit, the creditor must honor the offer so long as the individual continues to meet the criteria for the offer. Each prescreened mailing also must include instructions as to how the consumer can "opt out" of receiving prescreened offers in the future. Under the FCRA, a consumer can opt out of future prescreening from the three main credit bureaus simply by calling a single toll-free number.

Prescreening is a powerful tool in combating identity theft and other fraud. In this regard, the incidence of all fraud including identity theft is dramatically lower for credit card accounts when those accounts are obtained through prescreening rather than through other channels. Thanks to the national uniformity established under the FCRA, the benefits of prescreening as a fraud prevention tool are available across the country. It is critically important that the FCRA's national uniformity regarding prescreening be preserved.

Affiliate Sharing Provisions

The FCRA also regulates the sharing of information among affiliated entities. In this regard, the FCRA provides that information may be shared among affiliates and gives the consumer the right to opt out of the sharing of consumer report information. Affiliate sharing programs are increasingly used to control identity theft and other risks. For example, a card issuer's ability to thwart an identity thief may be enhanced significantly when the issuer can obtain information from its affiliated mortgage lender regarding a mortgage loan it has extended to the real individual whose name is being used on the identity thief's application. The FCRA currently establishes national uniform standards for affiliate sharing. The availability of affiliate sharing as an identity theft prevention tool would be significantly undermined if states were free to impose their own restrictions on affiliate sharing activities.

CONCLUSION

MasterCard and its members take our obligations to protect MasterCard cardholders against identity theft seriously. At MasterCard we have a team of experts devoted to designing and implementing new and better ways to protect MasterCard cardholders from fraud, including identity theft. These initiatives complement our members' activities to fight fraud and prevent identity theft. However, an important component of our collective efforts to protect consumers is the FCRA. As I have discussed, a critical tool in the fight against identity theft is the availability of accurate, reliable information about consumers. The availability of this flow of information is protected under the framework of a single uniform national standard established by the FCRA. I urge you to help ensure this information remains available by making the national uniformity under the FCRA permanent.

Thank you again for allowing me to appear before you today. I am happy to answer any questions you may have.