FIGHTING FRAUD: IMPROVING INFORMATION SECURITY

TESTIMONY OF JOHN J. BRADY
VICE PRESIDENT, MERCHANT FRAUD CONTROL
MASTERCARD INTERNATIONAL

Before the Subcommittee on Financial Institutions and Consumer Credit and
the Subcommittee on Oversight and Investigations of the
House Financial Services Committee

April 3, 2003

Good morning Chairman Bachus, Chairwoman Kelly, Mr. Sanders, Mr. Gutierrez, and members of the subcommittees. My name is John Brady and I am the Vice President for Merchant Fraud Control at MasterCard International in Purchase, New York. MasterCard is a global organization comprised of more than 15,000 financial institutions that are licensed to use the MasterCard service marks in connection with a variety of payments 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. It is my pleasure to appear before you this morning to discuss the important topic of fighting fraud and safeguarding financial information.

MasterCard takes its obligations to protect MasterCard cardholders, prevent fraud, and safeguard financial information very seriously. In fact, this issue is a top priority for MasterCard, and we have a team of experts devoted to maintaining the integrity and security of our payment systems. We are proud of our strong record of working closely with federal, state, and local law enforcement agencies to apprehend fraudulent actors and other criminals. Included among the federal law enforcement agencies with which we work closely are the U.S. Secret Service, the Federal Bureau of Investigation, the Federal Trade Commission, the U.S. Postal Inspection Service, and others. MasterCard also fields calls from local law enforcement every day. MasterCard believes its success in fighting fraud is perhaps best demonstrated by noting that our fraud rates are at historically low levels.

Information Security

Our success in protecting consumers and thwarting fraud is due in part to the constant efforts we undertake to keep our networks secure. MasterCard's information security program is comprehensive, and we continually update it to ensure that our program remains strong. Our member financial institutions also have information security protections in place including those

required under applicable banking law, such as the Gramm-Leach-Bliley Act (GLBA). For example, here in the U.S. our member financial institutions must adopt a comprehensive written information security program to protect their customers' personal information that includes administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These safeguards must be approved and overseen by the member financial institutions' board of directors. The safeguards must include an assessment of risk, procedures to manage and control risk, the oversight of service provider arrangements, and a mechanism to monitor and adjust the written information security program as necessary.

MasterCard also requires its member financial institutions to adhere to a comprehensive set of rules established by MasterCard to ensure the integrity and safety of MasterCard's payment system. For example, MasterCard's bylaws and rules require each member, and any third party acting on behalf of such member, to safeguard transaction and account information. Not only must our member institutions safeguard MasterCard transaction and account information, but our bylaws and rules require any merchant that accepts a MasterCard-branded payment device to prevent unauthorized access to, or disclosure of, account, cardholder, or transaction information.

Consumer Protection and Fraud Prevention

In addition to the strong information security programs in place, MasterCard remains constantly vigilant in an effort to detect potential data breaches or other potential fraudulent activity in order to mitigate any damage. MasterCard has an array of consumer fraud protections and anti-fraud tools, some of which I would like to describe.

Zero Liability and "Chargeback" Protection

First and foremost, MasterCard has taken steps to ensure that MasterCard cardholders are not responsible for fraudulent activity on their U.S. issued MasterCard accounts. In fact, we believe that our cardholder protections are among the most important consumer benefits a cardholder has as these benefits provide consumers with the security and comfort necessary to make the MasterCard system "the best way to pay for everything that matters." For example, MasterCard has voluntarily implemented a "zero liability" policy 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. Specifically, the Truth In Lending Act imposes a $50 liability limit for the unauthorized use of a credit card. Under the Electronic Fund Transfer Act a cardholder's liability for unauthorized use of a debit card can be higher. However, MasterCard 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 has greatly enhanced consumer confidence, including with respect to shopping on-line. A MasterCard cardholder can shop on-line and elsewhere with the confidence that he or she will have no liability in the event that his or her account number is used without authorization.

Cardholders who use MasterCard cards also gain additional protections against merchants who do not perform as expected. In many instances, if a cardholder uses his or her MasterCard card to pay for a product or service, and the merchant does not provide the product or service as

promised, the issuer can "chargeback" the transaction and thereby afford its cardholder a refund. This is a valuable consumer protection that is obviously not available with other forms of payment such as cash, checks, or travelers checks.

Card Security Features and Address Verification Service

It would seem ironic to say this, but MasterCard has worked to ensure that the account numbers alone on a MasterCard payment card do not hold much value. By this I mean that MasterCard has several systems in place to thwart a criminal who steals an account number, but steals little else. For example, it seems obvious but it is worth noting that if a thief fraudulently obtains a cardholder's account number, he or she would have a difficult time walking into a merchant to make a purchase because the thief would not have the card itself to present to the cashier.

MasterCard has worked hard to make it just as difficult for a criminal to make use of a credit 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 back of the credit card. MasterCard cards have the full account number printed on the back of the payment card, with an additional three digits which do not appear on the front 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 number for the credit card and can be used to ensure that the person presenting the credit card number actually has possession of the credit card—not just the account number.

A tool to fight similar 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 "name as it appears on the card" and billing address. At the time of payment, the merchant submits the consumer's name and 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 issuers of MasterCard 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 analyze certain trends. As just one example, MasterCard may identify countries where certain types of fraud may be unusually high. MasterCard and our member financial institutions use this data to take the appropriate precautions or otherwise react to the trends as necessary. 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 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 Alerts

MasterCard has developed a reliable and efficient system to notify the appropriate card issuers when MasterCard determines that MasterCard account numbers may have been compromised (*e.g.* fraudulently obtained by others). For example, if MasterCard learns that a card number may have been compromised, it will determine which bank issued the card bearing that account number and will notify the issuer that the account may be compromised. We have the capability to disseminate large numbers of account numbers to issuers in a short period of time through MasterCard Alerts. The issuer has the option to determine how best to address the problem, which may include increased monitoring of the affected account's activities to determine whether the account is being used fraudulently, or perhaps canceling the account and reissuing a new card and account number to the consumer. MasterCard also assists the issuer in monitoring the account usage in order to detect patterns of fraud.

Issuers Clearinghouse Service

MasterCard requires its member financial institutions 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. Furthermore, MasterCard members are required to access ICS in connection with each application to open a MasterCard

account. The ICS database allows MasterCard and its members to detect suspicious activity and to prevent consumer harms, such as identity theft. For example, the centralized ICS database would allow MasterCard and its 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 in a fraudulent manner. MasterCard members would be provided this data if they received an application with the same social security number or address and the member could evaluate it and take appropriate action.

A Recent Example of MasterCard's Efforts

I have described some of MasterCard's efforts to fight fraud and secure our systems. I would now like to discuss a recent example of how we address problems when they occur. There was a recent incident involving a data processor called Data Processing International (DPI). DPI was acting as a service provider to a MasterCard member bank in Ohio, which in turn was providing bankcard processing services to merchants. These services include processing the merchants' payment card transactions for submission into the appropriate payment systems. Earlier this year, DPI detected that someone had obtained unauthorized access to DPI's system. Although it is not clear at this point how much data the hacker successfully exported from the DPI system, we do know the hacker potentially had access to approximately 10 or 11 million Visa, Discover, American Express, and MasterCard payment card account numbers and expiration dates. Approximately 4 million of these account numbers were MasterCard account numbers.

Once DPI realized that someone had hacked their system, DPI took action. In addition, DPI and the bank quickly notified the U.S. Secret Service and the FBI as well as MasterCard and other affected payment card companies. MasterCard immediately took decisive action to protect its systems, its members, and, most importantly, MasterCard cardholders from fraudulent activity related to this breach. MasterCard interviewed the appropriate people at DPI, including the CEO, in order to determine the nature and scope of the breach. MasterCard gathered the card numbers involved and forwarded them via the MasterCard Alert system to the appropriate issuers. MasterCard also took steps to ensure that DPI had hired the appropriate third parties to investigate the situation, and MasterCard hired a third-party forensic firm to act on MasterCard's behalf during the investigation. MasterCard is continuing to review DPI's and the bank's information security program to ensure that they meet our standards.

MasterCard has been in ongoing contact with the issuers of the card numbers that may have been accessed. I am pleased to say that based on data we have analyzed, it does not appear that these numbers have been involved with unusual activity as a result of the breach at DPI. We believe that our success in mitigating any consumer harms as a result of the DPI hack is based on many factors. First, MasterCard has worked closely with law enforcement. Law enforcement has done a commendable job in investigating this breach and the investigation continues. Second, MasterCard's numerous anti-fraud initiatives, such as AVS and the added card security features, make it difficult for the hacker to make use of any account numbers he or she may have obtained without additional information.

Although it appears that the incident involving DPI has not resulted in any fraudulent activity, that is not to say that MasterCard has not encountered situations where an account is

used in fraudulent ways. In these instances, MasterCard works closely with the affected issuer to monitor the card usage data. MasterCard uses this data and works with the issuer and the appropriate law enforcement agency in order to apprehend the criminal. Of course, the issuer of the MasterCard card also closes the account and, under our Zero Liability policy, the cardholder is not held liable for any of the fraudulent activity on the account. The issuer also provides the cardholder with a new MasterCard card and account number.

Conclusion

MasterCard continually strives to provide its members and MasterCard cardholders with strong protections against fraud and similar activity. These protections include strong information security programs, comprehensive anti-fraud measures, and complete consumer liability protections. Although we are proud of our efforts to protect cardholders, members, and our payment systems against fraud, we will continue to develop new strategies and tools to thwart those who seek to do harm. Furthermore, we will continue to work hand in hand with law enforcement to apprehend perpetrators and continue to make MasterCard payment cards the best—and safest—way to pay for "everything that matters."