

CREDIT CARD DATA PROCESSING: HOW SECURE IS IT?

TESTIMONY OF JOSHUA L. PEIREZ **SENIOR VICE PRESIDENT AND ASSOCIATE GENERAL COUNSEL** **MASTERCARD INTERNATIONAL**

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

July 21, 2005

Good morning Chairwoman Kelly, Congressman Gutierrez, and members of the Subcommittee. My name is Joshua Peirez and I am a Senior Vice President and Associate General Counsel at MasterCard International in Purchase, New York. It is my pleasure to appear before you this morning to discuss the important topic of information security and I commend the Committee for holding this hearing. MasterCard is a global organization comprised of more than 23,000 financial institutions that are licensed to use the MasterCard service marks in connection with a variety of payments systems. It is important to note that MasterCard itself does not issue payment cards nor does it contract with merchants to accept those cards. Instead, those functions are performed by our customer financial institutions. The financial institutions that issue payment cards bearing the MasterCard brands are referred to as “card issuers.” The financial institutions that enter into contracts with merchants to accept MasterCard-branded cards are referred to as “acquirers.” MasterCard provides the networks through which the customer financial institutions interact to complete payment transactions and sets the rules regarding those interactions.

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 us, and we have a team of experts devoted to maintaining the integrity and security of our payment systems. We are also 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 U.S. Department of Justice (including 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 regularly. MasterCard believes its success in fighting fraud is perhaps best demonstrated by noting that our fraud rates are at historically low levels, well less than one-tenth of one percent of our volumes.

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. The MasterCard information security program is robust, and we continually update it to ensure that security remains strong. Our customer

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 customer 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 customer 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 customer 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 customer financial institution, and any third party acting on behalf of such customer, to safeguard transaction and account information. Not only must our customer 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.

MasterCard, along with other participants in the payment card industry, has also adopted the Payment Card Industry Data Security Requirements ("PCI Standards"). The PCI Standards apply to all customer financial institutions, merchants, and service providers that store, process, or transmit cardholder data. Compliance with the PCI Standards is mandatory as of June 30, 2005. The PCI Standards are comprised of twelve general requirements designed to: (i) build and maintain a secure network; (ii) protect cardholder data; (iii) ensure the maintenance of vulnerability management programs; (iv) implement strong access control measures; (v) regularly monitor and test networks; and (vi) ensure the maintenance of information security policies. For example, not only must our customer banks have comprehensive data security controls in place, but so must the merchants and service providers with which they contract. If a customer bank, or its merchants or service providers, fail to comply with the PCI Standards, the customer bank can be subject to significant penalties. In addition, MasterCard offers a multi-tiered, comprehensive set of global security services designed to help protect participants in our system from hack and attack. MasterCard designed these services to be a cost-effective diagnostic tool to allow participants to understand any systems vulnerabilities they may have. Furthermore, MasterCard also recommends actions that can be taken to reduce the potential systems vulnerabilities.

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, which are publicly available to merchants and consumers, 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 consumer cards. 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 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

MasterCard payment cards have significant security features designed to prevent criminals from counterfeiting our cards. For example, MasterCard cards have a highly sophisticated hologram. Our research suggests that this is not simple to duplicate in a credible manner. Furthermore, our cards include a magnetic stripe on the back. Not only does the magnetic stripe include such essential data as the payment card number, but it also includes additional information used to verify the card’s genuine issuance. The back of the card also includes a specialized signature panel with numbers engraved into it, making it more difficult to reproduce. Of course, issuers also add security features to the card, such as photographs of the cardholder or distinctive graphics and card designs.

We have also provided security features in the event a criminal obtains a cardholder’s account number. 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 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 card. MasterCard cards have the last four digits of the 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 can be used to ensure that the person presenting the card number actually has possession of the 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 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 a portion of the billing address into the MasterCard system to verify with the card issuer that the 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 service that provides added security when 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. By correctly entering 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 be declined.

“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 with the use of data provided by issuers of MasterCard regarding fraud-related transaction information. 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 customer financial institutions use this data to take the appropriate precautions or otherwise react to the trends as necessary. The SAFE program also helps us to identify potentially fraudulent actors relatively early in the process, before the problem escalates.

Transaction Monitoring

In addition to the proactive protections provided to prevent fraud from occurring, MasterCard and our acquirers have also implemented mechanisms to monitor transactions for potential fraud. For example, MasterCard's systems monitor transaction activity for signs of potential fraud, such as through monitoring merchant or cardholder transaction volume, the incidents of chargebacks, or other unusual activity. We often use this information to pinpoint suspected fraudulent activity so that merchants and banks can take the appropriate precautions.

MasterCard Alerts

One mechanism to place banks on notice is called 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, canceling the account and reissuing a new card and account number to the consumer, or perhaps notifying the cardholder. MasterCard also assists the issuer in monitoring the account usage in order to detect patterns of fraud.

Issuers Clearinghouse Service

MasterCard requires its customer financial institutions in the U.S. to participate in the Issuers Clearinghouse Service (ICS), a system built by MasterCard and Visa using data provided by card issuers regarding, among other things, the fraudulent use of consumer data. More specifically, MasterCard's U.S. customer institutions provide ICS with data regarding customer addresses, phone numbers, and social security numbers that have been associated with fraudulent activity. Furthermore, MasterCard customer financial institutions are required to access ICS in connection with each application to open a MasterCard account. The ICS database allows MasterCard and its customers to detect suspicious activity and to prevent consumer harms, such as identity theft. For example, the centralized ICS database would allow MasterCard and its customers 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 customer institutions would be provided this data if they received an application with the same social security number or address and the customer institution could evaluate it and take appropriate action.

The CardSystems Situation

I have described some of MasterCard's efforts to fight fraud and keep our systems secure. I would now like to discuss how we addressed the situation with CardSystems Solutions when it occurred. Several months ago, MasterCard and a few of our issuers noticed a small cluster of fraud which had no discernable source. As a clear pattern developed, MasterCard's security

team, working with issuers, was able to identify certain merchants as the source. These merchants shared a similar acquirer. MasterCard, working with the merchants' acquirer, was ultimately able to trace the pattern to a particular third party processor the acquirer utilized, CardSystems Solutions. Based on these factors, MasterCard required CardSystems' acquirer, Merrick Bank, to engage a MasterCard-approved data security firm to conduct a forensic analysis at CardSystems.

Upon being notified of the situation, CardSystems identified the presence of a malicious computer script in its system. The script was designed to export cardholder data without authorization. The Federal Bureau of Investigation was then contacted by CardSystems. Subsequently, the outside data security firm performed a forensic audit. The forensic investigation determined that (1) CardSystems was storing transaction information on its systems in violation of MasterCard rules; (2) there was a computer script found on one of CardSystems' systems, along with other serious security vulnerabilities; and (3) the forensic analysis uncovered specific evidence of a security breach of CardSystems' computer network. The preliminary results of the forensic audit were provided to the acquirer and to MasterCard in mid-June. Final results were provided in July. Based on these findings, it appears that information regarding approximately 68,000 different MasterCard payment card accounts and well over 100,000 payment card accounts of other brands had been exported from the CardSystems database.

MasterCard received a file of the affected account numbers on June 16. Following our established procedure, we used the MasterCard Alerts process to notify the banks affected as quickly as possible, which in this case began the very next day and was completed by Saturday, June 18. We also are working with our customer banks to monitor the potentially affected accounts to determine what additional steps, if any, are necessary. Given the circumstances of this case, MasterCard made the decision that a public disclosure of the event was warranted. Thus, we issued a press release to notify the public of the situation at CardSystems on June 17. I would like to stress that we provided broad public disclosure because it was the only responsible thing to do—not because we had a legal obligation to do so.

As demonstrated by our public announcement, our priority with respect to the CardSystems situation is to protect cardholders. With this in mind, we are now focusing our efforts on ensuring compliance with our data security requirements. For example, we recently sent letters to registered third party processors participating in our system reminding them of their need to comply with MasterCard's rules. Furthermore, we have required certification from the recipients of the letter that they have examined their systems and that such systems do not store sensitive cardholder information. We have also required CardSystems to bring its systems into compliance with our security requirements by August 31, 2005. We are holding weekly meetings with CardSystems to monitor its progress. If, however, CardSystems cannot demonstrate that they are in compliance by August 31, 2005, its ability to provide services to MasterCard customers will be at risk. Of course, we are considering penalties to be assessed with respect to the CardSystems breach as well.

Issuer Reimbursement

We understand the costs to consumers and to our card issuers associated with compromises of cardholder information. As I explained above, MasterCard has programs in

effect to ensure that U.S. cardholders are not liable for fraudulent transactions. MasterCard also has established a program under which our card issuers can obtain reimbursement for the monitoring and reissuance of cards as a result of a security breach.

Legislative Issues

We believe that Congress has established a solid framework for addressing issues relating to data protection. Based on our experience, we urge Congress to consider three improvements to law. First, we believe that stronger criminal penalties and more specific prohibitions should be provided for those criminals who compromise, or attempt to compromise, sensitive personal information. Second, we would like to work with Congress in establishing an appropriate consumer notification mechanism in situations where a data breach poses actual significant risks to consumers. Third, we believe that the law should establish clear data protection requirements for entities in possession of sensitive personal information if such entities are not already covered under the Gramm-Leach-Bliley Act. MasterCard looks forward to working with you as you tackle these important issues.

Conclusion

MasterCard continually strives to provide its customer financial institutions and 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, customer financial institutions, 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.”