STATEMENT OF

JOHN M. PERRY
PRESIDENT AND CEO

CARDSYSTEMS SOLUTIONS, INC.

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON OVERSIGHT
AND INVESTIGATIONS OF THE
COMMITTEE ON FINANCIAL SERVICES

HEARING ON
"CREDIT CARD DATA PROCESSING:
HOW SECURE IS IT?"

WASHINGTON, D.C.

JULY 21, 2005

Written Testimony of John M. Perry
CardSystems Solutions, Inc.
July 21, 2005

Good morning Madame Chairman and Members of the Subcommittee. Thank you for inviting CardSystems to appear before you today. My name is John Perry, and as President and CEO of CardSystems, I welcome the opportunity to discuss the issue of data security. More specifically, CardSystems believes this hearing will help inform the panel, cardholders and the public at large about the facts concerning the security incident perpetrated against us.

First and foremost, we truly regret this occurrence of data theft. We have repeatedly acknowledged our error, and are committed to making sure it does not happen again. As I will discuss in some detail, CardSystems has been working virtually non-stop since this incident, both to thoroughly diagnose what went wrong and to do whatever it takes to prevent any recurrence of this problem.

Make no mistake: exposure of information about one card is one too many. We will not be satisfied until we are confident that everything that can be done has been done to prevent this from happening again.

Despite these efforts, both Visa and American Express have informed CardSystems this week that they both will terminate us as a transactions processor as of October 31, 2005. We are disappointed with these actions and, in light of our diligent efforts to remediate, hope that both Visa and American Express will agree to discuss their decision with us and reconsider, lest we be forced to permanently close our doors.

Introduction

At the outset, let me offer some comfort and assurance to the Subcommittee that we believe what happened to us did not lead to consumer identity theft. The payment card system is designed so that processors like CardSystems do not have access to complete information, such as social security numbers, which could greatly facilitate identity theft.

Turning to the specifics of our situation, CardSystems identified a potential security incident on Sunday, May 22, 2005. Because of the criminal nature of the intrusion, we contacted the FBI on Monday, May 23. On May 25, we notified our sponsor, Merrick Bank.

Immediately after identifying the incident, CardSystems began reviewing all of its systems and hired an independent security firm to assess its operations and to recommend additional security measures. CardSystems has since adopted those recommendations and has installed upgraded security systems to protect them from being targeted again.

CardSystems also has been helping to facilitate all government inquiries, and will continue to do so. These inquiries include those being conducted by the FBI, the FDIC, and the Attorneys General of forty-six of the states, the District of Columbia and three U.S. territories.

Our cooperation with the FDIC includes assisting them in their continuing on-site review at our facilities which began in the third week of June. Also participating in this inquiry at CardSystems' facilities are the Office of Thrift Supervision (OTS), the Office of the Comptroller of the Currency (OCC), and the Federal Reserve.

The State Attorneys General have requested information from CardSystems regarding this incident, with a focus on potential

consumer harm, protection and notification. CardSystems has had multiple discussions with various representatives of the Attorneys General, and has provided and will continue to provide them with information they request as it becomes available to us.

We are still working with the payment card networks, as well as with our customers, who have stood by us as we have investigated this attack on our system. We hope that we may reach a favorable arrangement with Visa and American Express so that we can continue to stay in business.

About CardSystems Solutions, Inc.

CardSystems is headquartered in Atlanta, Georgia and its operating facilities are located in Tucson, Arizona. We are a relatively small business with approximately 115 employees.

CardSystems has been in operation for over 15 years, and has been processing payment transactions for more than 8 years. We currently handle payment transactions for over 110,000 small to mid-sized businesses, including restaurants, retail shops and local government entities. CardSystems, like other processors, routes

requests for transaction authorization from the point of sale (such as a card swipe terminal) to a payment card network, and then arranges for settlement of funds back to the merchant, although CardSystems does not actually receive or disburse those funds.

In order to gain access to the Visa and MasterCard networks, processors are required to obtain sponsorship from a Visa or MasterCard member bank. As I previously noted, CardSystems' sponsoring bank is Merrick Bank of South Jordan, Utah. Merrick Bank is a member of both Visa and MasterCard, and acts as a liaison between CardSystems and the card associations.

In addition to Visa and MasterCard, CardSystems authorizes transactions for American Express, Discover, JCB and Diners Club.

Data Security Standards in the Payment Card Industry

All merchants and service providers that store, process or transmit cardholder data are directed by the payment card networks to follow security standards. Before December 2004, these standards varied by network. Visa required compliance with its Cardholder

Information Security Program (CISP), which included a mandatory audit by a Visa-certified assessor.

In late Fall 2003, CardSystems was audited and certified by a qualified Visa CISP security assessor, Cable & Wireless. The Cable & Wireless audit, which concluded that CardSystems was unequivocally in compliance with Visa's CISP requirements, was reported to Visa in December 2003. The 2003 CISP audit determined that there were no deficiencies which were not covered by compensating controls. As a result, Visa qualified CardSystems as security-compliant in June 2004. Based on Visa's acceptance, CardSystems relied upon the CISP audit and certification as an assurance that it was compliant.

More recently, the payment card industry has developed a standard known as the Payment Card Industry Data Security Standard (or "PCI" Standard). The PCI Standard is based upon Visa's CISP, and was adopted by Visa, MasterCard, Discover, American Express, Diners and JCB in December 2004 to align their data security programs into a single uniform set of requirements.

The combined PCI Standard lists twelve requirements that all retailers, online merchants, data processors and other entities handling payment card data must meet, such as requiring installation and maintenance of a firewall and anti-virus software and regular virus definition updates. The PCI Standard also sets technology mandates, including requirements for secure storage of data. Entities that do not comply with the mandated security requirements may face sanctions.

Visa and MasterCard required all entities handling payment card data to comply with the PCI Standard by June 30, 2005. In light of CardSystems' recent incident, Visa and MasterCard had agreed to extend the time for CardSystems to conclude its PCI audit until August 31. CardSystems expects to be fully certified as compliant with the PCI Standard requirements at that time. While MasterCard continues to indicate that our compliance will allow us to remain an approved processor, Visa has this week changed its mind, and as of now plans to terminate us no later than October 31, 2005.

How the Security Breach Occurred

In September 2004, an unauthorized party placed a script (a sequence of instructions interpreted or carried out by another program) on the CardSystems platform (an underlying computer system on which application programs run) through an internet-facing application that is used by our customers to access data. In contrast to scripts, viruses and worms are programs or programming code that replicate indiscriminately and may result in file destruction.

This script ran on our system and caused records to be extracted, zipped into a file, and exported to an FTP site (similar to a web address). It was a sophisticated script that targeted a particular file type, and was scheduled to run every four days. Based on all of the forensic investigations conducted externally, by independent scans and investigations and by the payment card providers, we know of only one confirmed instance in which any data was exported, and that is the May 22 incident that has brought us here today.

The offending script searched our computer servers for records with track data (the data on a card's magnetic stripe, which is affixed

to cardbacks and contains identifying data). The most complete information that could have been obtained for any one cardholder would have been that person's name, account number, expiration date and CVV code (contained in the magnetic stripe). Since this data does not include the cardholder's social security number, we believe that there is virtually no risk of identity theft resulting from this intrusion.

The data stored in the files that were confirmed to have been exported by the script consisted of transactions which were not completed for a variety of reasons. This data was stored for research purposes in order to determine why these transactions did not successfully complete. As we have repeatedly acknowledged, our error was that the data was kept in readable form in violation of Visa and MasterCard security standards. As of May 27, 2005, track data is no longer stored by CardSystems.

Number of Consumers Impacted by the CardSystems Security Breach

As the result of the extensive forensic analysis in which we have participated, we know for certain that three files were wrongfully

removed from the CardSystems platform. Of these three files, one was empty, one contained about 4,000 records, and the third contained approximately 259,000 records. The total 263,000 records correspond to 239,000 discrete account numbers. The only records that are confirmed to have left the CardSystems platform were those 263,000 records (representing the 239,000 unique account numbers) that were exported on May 22.

From the card numbers extracted from CardSystems' archived data, the card associations have been able to determine which card issuing banks were affected. By virtue of the rules governing the payment card industry which were enacted in part to protect the privacy of cardholder information, CardSystems does not possess the data that would enable it to notify cardholders who may have been impacted by this incident. Instead, the card issuing banks, through their direct relationship with cardholders, have the complete records that include the names and addresses of cardholders.

So far, out of all of the account numbers that may have been affected, we have not been notified of any that have been used

fraudulently. As I have indicated, the security systems in place in the payment card industry are set up to ensure that minimum cardholder account information is provided to payment processors like us. This also means that CardSystems has no access to the information which would provide us the means to directly monitor consumer fraud. The payment card networks and the card issuing banks, on the other hand, do have such means, and they are continuing to closely monitor cardholders' accounts.

Steps CardSystems is Taking to Prevent Any Future Security Breach

Almost immediately after the breach was detected, CardSystems contacted an outside security solutions firm located in Tucson to identify any additional vulnerabilities from further outside intrusion, and to insure that the actions taken by CardSystems personnel shortly after the intrusion was discovered would prevent the script from continuing to run.

Merrick Bank also retained security assessment and forensic experts immediately after Memorial Day. The role of these experts was to identify the source of the compromise, ensure that there was no

risk for continued compromise, and recover as much data as possible to identify the full extent of the breach.

Merrick's experts determined that the breach resulted in the installation of a script onto CardSystems' computer system through an internet-facing web application in September 2004.

CardSystems continues to cooperate with the inquiries of the regulatory agencies, the FBI, Merrick Bank and the card associations. We continue to focus intensely on remediation and implementation of best practices security as defined by outside security assessment and forensic experts. We have been particularly focused on complying with Visa CISP and PCI standards. For example, CardSystems no longer stores track data, and all track data is now otherwise masked or rendered unreadable.

Based on CardSystems' efforts to address the situation and to ensure that it does not recur, Visa and MasterCard agreed to extend the deadline for CardSystems' PCI security compliance to August 31, 2005. In conjunction with our efforts to achieve PCI security compliance by August 31, we have selected AmbironTrustWave, a

Qualified Data Security Company (QDSC), to perform our official PCI Standard assessment. The assessment will enable us to mitigate risk by validating compliance with the PCI Standard, and therefore with the data security programs of Visa, MasterCard, Discover, American Express, Diners and JCB.

Conclusion

As Chairman Spencer Bachus noted in his opening statement before the Subcommittee on Financial Institutions and Consumer Credit on May 18, 2005, "[e]ven the most prudent company can become the victim of a hacker or other criminal." While we agree with this, CardSystems is learning from this breach and improving the way we do business. CardSystems remains committed to protecting its customers and to ensuring the security of cardholder data.

Madame Chairman, this Subcommittee is to be commended for dedicating its time and attention to the important issues we are discussing today. Thank you for allowing us to participate.