

House Financial Services Committee
Subcommittee on Oversight and Investigations
Hearing: "Credit Card Processing: How Secure Is It?"
July 21, 2005

Written Statement of
Zyg Gorgol, Senior Vice President, Fraud Risk Management
American Express Company

Chairwoman Kelly, Ranking Member Gutierrez, members of the Subcommittee, my name is Zyg Gorgol and I am Senior Vice President of Fraud Risk Management at American Express. American Express Company was founded in 1850 and is today a diversified worldwide travel, network and financial services provider. We are leaders in charge and credit cards, Travelers Cheques, travel, network services and international banking.

I appreciate the opportunity to testify today about the recent data security breach at CardSystems Solutions, Inc. and its impact on American Express Cardmembers. We view this breach with great concern and have taken steps to protect any Cardmembers who may have been affected by it. I also want to comment today about American Express' data security standards for merchants and third-party processors. We believe our work in this area is a critical element in helping to ensure that sensitive Cardmember information that is processed on the American Express network remains secure.

Background

American Express operates what is often referred to as a "closed-loop" network. American Express issues charge and credit cards to customers, and also has direct arrangements with merchants who accept American Express Cards. This can be distinguished from an open network arrangement, where the entity that maintains arrangements with merchants for card acceptance is typically not also the card issuer. In an open network environment, the network provider or association serves as a conduit between the issuer and the acquirer.

In terms of data security, which is the focus of this hearing, there is nothing technically more secure in an open or closed loop network. However, we at American

Express have through the years used what we learned from our closed loop environment to build state-of the-art systems to detect and prevent fraud. I believe our fraud prevention efforts have benefited significantly from the valuable information our closed loop network provides.

American Express also operates a Global Network Services business where we partner with select banks to issue cards on the American Express network. In this case, our partners issue cards on the American Express network, while we continue to maintain the merchant relationship. In the United States, MBNA, Citibank, Juniper Bank, and USAA have signed up to issue American Express Cards to their customers.

Payment Card Industry Data Security Standards

The Payment Card Industry Data Security Standards (referred to as the PCI Standards) provide an industry-wide approach to safeguarding charge and credit card customer data. The PCI Standards were developed by a cross-industry working group that included American Express, Visa U.S.A., MasterCard International, Diner's Club, JCB, and Discover.

Specifically, the PCI Standards apply to any merchant or processor that handles any cardholder data. The Standards require merchants and processors to (1) build and maintain a secure network; (2) protect cardholder data; (3) maintain a vulnerability management program; (4) implement strong access and control measures; (5) regularly monitor and test networks; and (6) maintain an information security policy. With respect to protecting cardholder data, the PCI Standards specify encryption standards to protect stored data and transmission of cardholder data and sensitive information across public networks. In addition, the Standards specify that merchants and processors must not

store the full contents of any information from the magnetic stripe on the back of the card or the validation identification code that appears on the card.

While American Express fully endorses these Standards as an appropriate industry baseline standard for data security in the payments industry, we recognize that the PCI Standards do not resolve all issues. Indeed, in the case of the data security breach at CardSystems, the PCI Standards apparently were not followed in a number of important ways.

CardSystems Breach

CardSystems Solutions processes less than one percent of American Express Card transactions. Upon learning of the breach at CardSystems, we began an extensive investigation to determine any impacts on American Express Cardmembers. We also followed our practice of flagging potentially affected accounts and putting additional security and fraud prevention measures in place for those accounts. We are continuing to closely monitor those accounts for any suspicious activity on an ongoing basis.

Based upon our investigation into the CardSystems breach, in which we worked directly with the computer forensics firm Cybertrust, we have determined the following:

- The CardSystems database that was accessed by unauthorized persons contained records of approximately 40 million charge and credit card accounts -- only a small percentage, approximately four percent, of these were American Express Card accounts.
- Our analysis indicates that information relating to approximately 12,000 American Express Card accounts in the CardSystems database appears to have been accessed by unauthorized persons.

- Although the information relating to these 12,000 accounts included the card account number and expiration date, it did not include any personally identifiable information of American Express Cardmembers, such as name, address, or telephone numbers, nor did it include any other sensitive personal information, such as Social Security numbers or driver's license numbers.
- While we have been closely monitoring these accounts, we have not detected any increased incidences of fraud on these 12,000 accounts. We are continuing to monitor these accounts for any suspicious activity.

According to reports from CyberTrust and other published reports, the intrusion into the CardSystems database was made possible by the failure to have appropriate computer intrusion protection and detection measures in place. This was exacerbated by the storage on CardSystems' database of credit and transaction data that should have been purged from its records, and it was further exacerbated by the failure to encrypt the stored data. Such actions would violate both American Express' data security policies and the PCI Standards.

We take these violations very seriously. Based on our current analysis, we have notified CardSystems of our intention to end the processing relationship with them.

Fraud Detection and Prevention

American Express employs sophisticated monitoring systems and controls to detect and prevent fraudulent activity. Historically, this has been an area of emphasis for American Express. Over the last several years, we have invested tens of millions of dollars to enhance our fraud prevention capabilities to better protect Cardmembers. It is

in our interest to do so, since by minimizing fraud we reduce the considerable costs to us and the industry each year from fraudulent activity. If fraudulent charges are placed on an American Express Card account, we stand behind our Cardmembers. American Express Cardmembers are not held liable for fraudulent charges.

Since 2001, both the transaction volume and charge volume on our network has increased substantially. During this period the overall fraud rate has declined significantly. We are constantly adjusting our fraud prevention techniques to adapt to the changing strategies of fraudsters. While we do not disclose the details of our fraud prevention measures in order to prevent criminals from having knowledge of our procedures, steps we take to protect our Cardmembers include the following:

- Customer Password: Every American Express Cardmember is asked to establish a password in the voice response system, providing an additional level of authentication for account maintenance.
- Charge Verification: On transactions above \$200, if fraud is suspected by a merchant, the merchant can contact American Express and we will speak directly with the Cardmember to authenticate the transaction.
- Card Identifier Digits/Card Identification Number (CID): The CID number provides an additional level of verification for merchants (both online and off). This 4-digit number is printed on the front of all American Express Cards (also referred to as CVV2 or CVC2 as a 3 digit number on the back signature panel of bank cards).
- Zip Code Verification: This provides for an additional level of authentication at the point of sale by enabling merchants to ask

Cardmembers to provide their zip code, which may be a piece of information a fraudster would not have.

- Automatic Address Verification (AAV): This verifies for the merchant that the address provided by the customer matches the billing address on file with American Express. Our AAV technology is very sophisticated and is considered a “best practice” in the industry.

In the case of the CardSystems breach, we have implemented additional security and fraud prevention measures for all of the American Express Card accounts with information stored on CardSystems’ database. In addition to our normal fraud detection procedures, we continue to closely and more intensely monitor these particular accounts for any suspicious activity on an ongoing basis.

If we detect any unusual activity on these accounts that may be fraud, we will contact the customer. In many instances, we detect fraud well before a customer becomes aware of any unusual activity on an account, and we proactively reach out to affected customers. If we verify with the Cardmember that fraud has occurred we will replace the Card.

If we learn that any merchant, processor, or any other participant in the payment card transaction cycle may have been subject to a breach, we quickly apply additional anti-fraud measures. It is important that we learn about any potential breach promptly so that our additional fraud detection and prevention measures can be implemented as quickly as possible. It is also important to reiterate that American Express Cardmembers are not held liable for any fraudulent charges.

Identity Theft Prevention

It is important to distinguish between two different types of criminal activity: credit card fraud and identity theft. Fraud occurs when a criminal places a fraudulent or unauthorized charge on a card account. Identity theft occurs when a criminal uses information about a person to open a new account in the victim's name or to take over use of an existing account by changing, for instance, the name or billing address on the account. Typically, a criminal needs access to sensitive personal information, such as the date of birth, a driver's license number, or a Social Security number, to commit identity theft. This distinction becomes important when analyzing particular data elements that may have been compromised and the harm to customers that might result from the misuse of compromised information.

In order to help consumers detect and prevent identity theft, American Express provides free Identity Theft Assistance to all American Express Cardmembers. This assistance includes access to representatives who are on call 24 hours a day, seven days a week, to offer help on how to protect against identity theft; it also suggests steps Cardmembers can take if they notice any suspicious activity on their accounts. American Express Cardmembers can also sign up to receive alerts for any irregular account activity, via cell phone, PDA, or e-mail. This alerts program is available at no cost to our Cardmembers.

In addition, American Express has a long history of working externally with consumer and privacy advocate organizations to educate consumers on issues such as information security, fraud and identity theft. Most recently, we hosted a roundtable discussion on identity theft that included participation from the U.S. Department of

Treasury, FBI, FTC, and the Council of Better Business Bureaus. We also published a consumer brochure in cooperation with the California-based Privacy Rights Clearinghouse and the Identity Theft Resource Center on how consumers can protect themselves against identity theft and the steps consumers can take if they become victims. We are also major supporters of the National Consumers League online Fraud Information Center and are active members of the Alliance Against Fraud in Telemarketing and Electronic Commerce.

Later this year, we are co-sponsoring a summit to address the growing problem of "phishing." One concern is that "phishers" will take advantage of known data breaches to send out counterfeit notifications seeking personal sensitive information. Summit participants will include consumer advocates, federal and local law enforcement officials, internet service providers, technology companies and academics. As has been our tradition, we will continue to work in cooperation with consumer advocates to increase consumer awareness of these issues and identify solutions.

Customer Notification

American Express supports a consistent and effective national notification standard as an important component of data security response program. Notification to consumers is appropriate when compromised information is reasonably likely to be misused to the harm of the consumer and the notification will provide the consumer a meaningful opportunity to take appropriate steps to protect against that harm. We believe the current notification regime could be improved by addressing three important areas.

First, there should be an appropriate threshold to trigger notification. The intent of notification is to prevent harm to the customer; over-notification can result in

consumers becoming desensitized to the many notices they might receive. As a result, consumers could pay insufficient attention to a significant incident and fail to act when preventive measures are necessary.

Second, we believe that notification requirements must take into account the scope of the particular information that has been compromised and the harm to consumers that could result from the misuse or potential misuse of compromised information. Notifications are useful to consumers if they communicate the significance and likelihood of the potential harm caused by a breach and provide guidance on how to prevent or mitigate the potential harm. All compromises are cause for concern, but not all compromises present the same potential consequences or potential harm to consumers.

Third, a consistent and effective national standard for notification serves consumers best. It will enable uniform application across the country and lead to uniform enforcement by regulators and law enforcement authorities. It is undesirable and impractical to have a patchwork of consumer notification requirements that vary by state or entity.

Recommendations

In light of these recent data security breaches, we believe there are some tangible steps that can be taken to better protect consumers. First, payment card transactions are handled by regulated and unregulated companies, and we recommend that Congress extend Gramm-Leach-Bliley (GLBA)-like safeguard standards to those companies involved in processing card payments that are not currently subject to these safeguards.

Sensitive customer information should be consistently protected as it proceeds through the payment card transaction cycle. All participants in the payment card

transaction cycle that possess or control sensitive customer information should have a direct legal obligation to implement appropriate data security measures to safeguard that information.

We would also suggest that appropriate cross-industry measures be implemented to certify, and verify on an ongoing basis, adherence to the PCI Standards by all entities in the payment card transaction cycle. This effort should include processes to notify, promptly and simultaneously, all potentially impacted issuers and network providers if a breach is discovered.

We also support increased criminal penalties for those who steal sensitive personal information and those who commit computer fraud. While we recognize that it is often very difficult to catch those who commit this type of fraud, we believe that enhanced criminal penalties would provide law enforcement additional tools to go after fraudsters and is an important step in helping to combat this activity.

The issues discussed here today are complex; appropriately addressing these issues will require dialogue among legislators, regulators, law enforcement agencies and the industry. By working together, we can provide the protection consumers need while maintaining the convenience of using charge and credit cards that consumers have come to rely on.

Conclusion

I want to assure the Subcommittee that American Express is strongly committed to protecting the security of our Cardmembers' personal information. It is clear that recent events have raised the public's concern regarding the security of their personal information, and how this information may be compromised and potentially misused.

We share this concern and are constantly working to protect the security of our Cardmembers' information so that when a customer makes a transaction using an American Express Card, they have confidence that it will occur in a safe and secure manner. Data security is a critical issue for our entire industry, and we are committed to working with all interested parties to ensure a secure payments environment.

We appreciate the opportunity to share our views on this issue, and we look forward to working with you and other members of the Financial Services Committee. This concludes my prepared testimony. I would be happy to answer any questions that you may have.