

STATEMENT
OF
STEVE RUWE
ON BEHALF OF
VISA U.S.A. INC.
BEFORE THE
SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS
OF THE
COMMITTEE ON FINANCIAL SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

Credit Card Data Processing: How Secure Is It?

July 21, 2005

Chairwoman Kelly and Members of the Subcommittee, my name is Steve Ruwe. I am the Executive Vice President of Operations and Risk Management for Visa U.S.A. Inc. (“Visa”). Visa appreciates the opportunity to address the important issues raised by today’s hearing on information security.

The Visa Payment System, of which Visa U.S.A. is a part, is a leading consumer payment system, and plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud.

Visa commends the Subcommittee for focusing on the important issue of information security. As the leading consumer e-commerce payment system in the world, Visa considers it a top priority to remain a leader in the development of technology, products and services that protect consumers from the effects of information security breaches. As a result, Visa has long recognized the importance of strict internal procedures to protect the customer information of Visa’s members.

Visa has substantial incentives to maintain strong security measures to protect customer information. Cardholder security is never just an afterthought in the transaction cycle at Visa. For Visa, it’s about trust. Our goal is to protect consumers, merchants and our members from fraud by preventing fraud from occurring in the first place. This commitment to fighting fraud extends to Visa’s Zero Liability policy which protects Visa cardholders from any liability for fraudulent purchases. Because the financial institutions that are Visa members do not impose the losses for fraudulent transactions on their cardholder customers, these institutions and, in some cases, the merchants that honor

Visa cards, incur costs from fraudulent transactions. These costs primarily are in the form of direct dollar losses from credit that will not be repaid to card issuers. Typically, these losses are borne by the card issuer; however, if the merchant fails to follow proper authorization procedures for face-to-face transactions, costs may be passed back to the acquiring bank or the merchant that participated in a fraudulent transaction. For Internet, telephone and mail transactions, merchants are generally responsible for unauthorized purchases; however, Visa provides merchants with a number of tools to prevent fraud, and, by using Verified by Visa, merchants can shift these losses to the card issuing bank. In order to protect its members from these costs, Visa aggressively protects the customer information of its members.

Visa's Information Security Programs

Visa employs a multi-faceted approach to combat account fraud and identity theft. Visa has implemented a comprehensive and aggressive customer information security program known as the Cardholder Information Security Program ("CISP"). This security program applies to all entities, including merchants, that store, process, transmit or hold Visa cardholder data, and covers enterprises operating through brick-and-mortar stores, mail and telephone order centers or the Internet. CISP was developed to ensure that the customer information of Visa's members is kept protected and confidential. CISP includes not only data security standards, but also provisions for monitoring compliance with CISP and sanctions for failure to comply. Visa has been able to integrate CISP into the common set of data security requirements used by various credit card organizations without diluting the substantive measures for information security already developed in

CISP. Visa supports this new, common set of data security requirements, which is known as the Payment Card Industry Data Security Standard (“PCI Standard”).

Visa also provides sophisticated neural networks that flag unusual spending patterns for fraud that enable our members to block the authorization of transactions where fraud is suspected. When cardholder information is compromised, Visa notifies the issuing financial institutions and puts the affected card numbers on a special monitoring status. If Visa detects any unusual activity in that group of cards, Visa again notifies the issuing institutions, which begin a process of investigation and evaluation of the need for any card re-issuance.

In addition to the CISP and the neural networks that monitor spending patterns, Visa has implemented a variety of security measures designed to detect and prevent particular fraudulent transactions:

- Visa’s Address Verification Service (“AVS”) matches shipping and billing addresses and other information to confirm that a transaction is valid.
- Visa maintains an exception file comprised of a worldwide database of account numbers of lost or stolen cards or other cards that issuers have designated for confiscation or other special handling. All transactions processed through the Visa system have the account numbers checked against this exception file.
- The Cardholder Verification Value (“CVV”) is a unique three-digit code included in the magnetic strip located on the back of all Visa cards. The

CVV is electronically checked during the authorization process for card-present sales to ensure that a valid card is present.

- The CVV2 is a unique three-digit code printed on the signature strip on the back of all Visa cards. These codes help merchants confirm that cardholders are in possession of the actual card. Online merchants or telephone merchants conducting transactions when the card is not present can verify that their customers have the actual card by requesting the customer to provide the CVV2 number.
- Verified by Visa both protects customers and allows merchants to avoid charge back costs in online transactions by having cardholders authenticate their identities while shopping online. Its password protection reduces the potential for fraud over the Internet.
- Advance Authorization provides an instantaneous analysis of the potential for fraud at the time of a transaction.

As a result of these strong security measures, fraud conducted within the Visa system is at an all-time low of five cents for every \$100 worth of transactions.

In addition, only yesterday Visa and the U.S. Chamber of Commerce announced a new nationwide data security education campaign that will involve both the payments industry and merchants in the fight to protect cardholder information and reduce fraud. Visa believes that all parties who participate in the payment system share responsibility to protect cardholder information.

Security Breach Incident Involving The Payments Processor

Visa was recently informed by payments processor CardSystems Solutions, Inc. (“CSSI”) about an unauthorized intrusion into CSSI’s computer system. As soon as Visa was aware of this potential breach, Visa immediately began working with the processor, law enforcement and affected member financial institutions to prevent card-related fraud. While the initial investigation was underway, Visa respected standard law enforcement protocol regarding keeping information about the investigation confidential.

After being notified by the processor, Visa’s rapid response quickly went to work with our member banks to monitor and manage potentially exposed accounts. Some of our member banks have their own fraud monitoring systems to supplement the Visa monitoring systems.

Visa notified all of the potentially affected card-issuing banks and provided them with the necessary information so that they could monitor the accounts independently, and, if necessary, advise customers to check their statements or cancel and reissue cards to their customers. The card-issuing financial institutions that are members of the Visa system have the direct relationship with their customers who carry Visa cards, and because of Visa’s Zero-Liability policy for cardholders, bear most of the financial loss if fraud occurs. These institutions are in the best position to determine the appropriate action with respect to each customer account that might have been affected by a security breach such as the CSSI breach.

To date, we have determined that approximately 22 million Visa card numbers from the CSSI database were put at risk. In many of those cases, CSSI, by its own admission, knowingly and improperly retained magnetic stripe information that can be

used to help create counterfeit cards. This action by CSSI was a clear violation of the CISP. Visa believes that there is no valid reason for merchants or acquirers to retain security code information. Retention of this information in a database makes the database a much more attractive target for criminals and would require more robust security and additional costs. As a result of CSSI's failure to follow Visa security requirements, Visa is terminating CSSI's ability to act as a processor for Visa members.

Significantly, the information that was retained by CSSI did not include the cardholder's date of birth, address, social security number or driver's license number. As a result, Visa believes that the information involved in this incident cannot be used to commit identity fraud against any of the potentially affected individuals in which a criminal opens a new account in the individual's name.

Protecting our cardholders was—and remains—Visa's primary goal throughout the process of responding to this incident. We are actively monitoring the situation on a real-time basis, using our state-of-the-art fraud-fighting technologies, such as Advanced Authorization and Visa's neural networks. Visa will continue to protect for our cardholders and assist law enforcement in their efforts to find those who are responsible for this crime.

Pending Data Security Legislation

Visa has not taken a position on specific pending legislation in this area. In general, we favor federal legislation that would extend reasonable risk-based security and notification requirements to all entities that have sensitive customer information. We also believe that these policies should be consistently applied nationwide to avoid a clash

of conflicting state laws in this area. Finally, we favor stronger penalties for identity theft and additional resources for state and local law enforcement to combat identity theft.

Thank you, again, for the opportunity to present this testimony today. I would be happy to answer any questions.