Statement of

Carlos Minetti

Discover Financial Services

Before the

Subcommittee on Oversight and Investigations

of the

Committee on Financial Services

United States House of Representatives

July 21, 2005

Madam Chairman and Members of the Subcommittee, thank you for inviting Discover Financial Services[1] to share our views on the issue of data security breaches affecting credit card information.

As Discover's Executive Vice President for Cardmember Services, I am responsible for operations, customer service and risk management. This includes oversight of Discover's information security and anti-fraud efforts.

[1] Discover Financial Services, Inc., headquartered in Riverwoods, IL, is a business unit of Morgan Stanley. It operates the Discover Card with more than 50 million Cardmembers, the Discover Network with more than 4 million merchant and cash access locations and the PULSE ATM/Debit network currently serving more than 4,000 banks, credit unions and savings institutions.

The subject of today's hearing – the security of financial information - is very important to financial services providers and the consumers we serve. Security breaches and the appropriate responses to them are issues that must be addressed in a consistent manner so that consumers nationwide have the same protections and confidence in the security of their financial information no matter where they live.

Security Breach Prevention

Discover works hard every day to prevent customer information from falling into the hands of individuals who would hope to use it for criminal purposes, like account fraud or identity theft. Identity theft involves unauthorized use of personal information (such as an individual's name, address and Social Security number) to open *new* accounts with financial institutions or other service providers in the name of the victim, but without the knowledge of the victim. Identity theft can result in frustrating efforts to reclaim one's identity and other costly consequences.

Account fraud, on the other hand, involves the use of an *existing* credit card without authorization of the cardholder to make purchases or obtain cash advances. The real victim of this crime is generally not the consumer whose account was involved, but rather the credit card issuer. Federal law limits consumers' responsibility for unauthorized transactions (Discover customers' liability for fraudulent transactions is zero), and consumers can generally have these transactions erased from their accounts with little difficulty.

At Discover, we continually review, and if necessary upgrade, internal efforts to ensure that access to information is limited to individuals who have a legitimate business need to see it; that employees are adequately screened, trained and monitored; that computerized information is maintained securely; that the identity of card applicants is verified; and that customer accounts are monitored for signs of suspicious activity. Financial institutions, like Discover Bank, the issuer of our cards, are subject to the Gramm-Leach-Bliley Act's information security standards and the Interagency Guidance on security breach response programs. The FDIC examines Discover Bank for compliance with those standards.

Protection of Discover Cardmembers

Discover monitors its 50 million Discover Cardmember accounts nationwide for signs of unauthorized activity, and notifies Cardmembers in the event of suspected account misuse. We provide Cardmembers with information and educational messages about safeguarding personal information and with tools to enhance the security of that information.[2] Our Customer Service Representatives are available 24 hours a day, every day, to assist all Discover Cardmembers with inquiries or concerns about information security and to resolve issues about unauthorized transactions promptly. These representatives are empowered to address customer inquiries expeditiously, without

[2] For example, Cardmembers who shop over the Internet can use Discover's secure online shopping service that generates a single-use card number to be used in lieu of the Discover Card account number.

requiring the customer to make multiple calls, navigate through menus of options, or listen to lengthy recorded messages.

In the event that a consumer believes that he or she is a victim of identity theft involving a Discover account, we assign a Personal Fraud Specialist to assist the individual in working with creditors, law enforcement personnel, and consumer reporting agencies. Consumers appreciate the ability to stay in contact with the same Specialist throughout the process of resolving identity theft issues.

A 2005 "Identity Fraud Safety Scorecard for Credit Card Issuers" conducted by Javelin Strategy & Research ranked Discover first in "overall card safety features" and first for "detection safety features." [3]

Data Held by Merchants, Their Processors and Other Service Providers

As Discover and other credit card issuers and networks improve internal defenses against computer hacking and other threats to the information we hold, criminal enterprises have begun to focus on what they may see as "soft targets." These include merchants and service providers that accept credit cards, and the third party vendors that they use to process payment information and manage their businesses.

[3] 2005 Issuer Scorecard" by Javelin Strategy & Research (www.javelinstrategy.com). Javelin's study scored issuers on 38 categories of capabilities for fraud prevention, detection and resolution.

The millions of businesses that accept credit card payments include the largest American companies that accept cards for billions of dollars in sales and account for a significant volume of total retail sales (and credit card transactions). The largest merchants are the most attractive targets for would-be identity thieves or fraudsters, but they also tend to have the most sophisticated information processing systems and data protection regimes, backed up by internal security teams. Cards are also accepted by millions of smaller entities, some of them part-time businesses operated by a single individual. Although smaller merchants may not have similar information security systems or resources, they are also less likely to be targeted by large scale ID theft or fraud rings because the volume of data they hold may simply not be worth the effort involved in stealing it. In evaluating the adequacy of efforts to safeguard personal financial information held by merchants and service providers, it is important to be mindful of these differences, so that resources are allocated appropriately and unnecessary and unworkable approaches are avoided.

Discover's contracts with the merchants that accept Discover Network cards requires them to safeguard account information, and to use it only for specified purposes related to payment processing. The merchants agree that they will not store the full information encoded in a card's magnetic stripe or the three-digit card validation code, and that they will destroy or purge obsolete transaction data. Merchants also commit to providing access to the data only to processors, software vendors, and other agents or service providers that have security standards that comply with these requirements.

The Discover Network has direct relationships with each of the merchants and service providers who accept Discover Network cards. Discover communicates regularly with these merchants to remind them about our data security requirements, inform them about emerging threats and software or other vulnerabilities, and provide information about resources and technical assistance for enhancing data security. Discover provides its merchants with tools and services that can be used to validate their compliance with our requirements for secure information processing and transmission. For online merchants, who are particularly vulnerable to security breaches, our Merchant Operating Regulations give the Discover Network the right to perform periodic data security scans to ensure that the merchant remains in compliance with Discover's security and encryption requirements.

Discover reviews merchant and processor data daily. This helps to pinpoint areas of vulnerability by identifying suspicious transactions and patterns of activity. It is a risk-based approach that allows us to focus compliance efforts where they are needed, and is the basis for identifying merchants or processors for targeted responses in the form of alerts and inquiries, transaction monitoring, and physical audits.

Discover's security requirements, which we revised in 2004, are consistent with the "Payment Card Industry Data Security Standard." This is an industry-wide standard for the protection of account data that allows merchants to use the same procedures regardless of the cards they accept or the processors and agents they use. It also allows

merchants to use a single set of security standards in assessing the adequacy of their efforts to safeguard information about their customers' payment card transactions.

Discover's Security Breach Response Measures

Discover's response to data breaches are consistent with standards specified in the Interagency Guidance on Response Programs and a growing number of state laws. We also have a strong financial interest in addressing security breaches, because as noted previously Discover, and not our Cardmembers, absorbs the losses from fraudulent transactions. When information obtained by virtue of a data breach is used to make purchases or cash withdrawals on a Discover account, we promptly delete the charge from the account and absorb the loss.[4]

Because we operate both a large merchant network and issue the Discover Card, we are often able to learn about computer hackings and other signs of data compromises when they first occur. In fact, Discover was the first network to uncover evidence of data compromises in many of the recently publicized security breaches involving large merchants and payment processors.

[4] The notion that card issuers are not concerned about data breaches because the chargeback process insulates them from financial loss is simply untrue. We do not routinely charge back purchases to merchants who accept a stolen or counterfeit card or process a transaction not authorized by the cardholder unless the merchant fails to follow card authentication procedures (e.g., obtaining the three-digit security code for online or telephone transactions where no card is presented).

An internal Discover Task Force is responsible for maintaining effective procedures for addressing security breaches. Comprised of individuals from both our card issuing and payment network businesses, the Task Force meets regularly to discuss security issues, and is convened in the event of a breach to assess the appropriate responses. It has developed response action plans to address different forms of data compromise. The Task Force is also responsible for the development of customer education information regarding account fraud and identity theft.

Upon learning of a data security breach that may affect Discover Cardmembers (such as the incident involving credit card data held by CardSystems Solutions, Inc.), we immediately commence an investigation. We first ascertain the type of information involved to determine whether the data could be used to commit identity theft or otherwise harm the customer. For example, did the incident involve unauthorized access to account numbers? account numbers and security codes? customer names and addresses? Social Security numbers? We also identify the specific accounts that were affected, information that we need to monitor those accounts and take further action if necessary, such as contacting our customers or closing accounts.

Where the breach is external (e.g., data held by merchant or processor) we must rely on information from the affected companies. We work with these companies and with third party investigators to evaluate the impact on Discover Cardmembers. We gather information and assist the entity whose security was compromised in retaining (and sometimes in paying for) the services of forensic investigative firms that specialize in

evaluating data breaches. We also work with other card networks when their account data is affected.

If we determine that the data that was accessed without authorization is likely to result in customer harm, we notify affected Cardmembers in accordance with the Interagency Guidance and the requirements of state laws. We also take further actions that may be necessary to prevent harm, such as further monitoring or the closing of accounts.[5] Discover coordinates its efforts with the FDIC and with law enforcement personnel who may be investigating the incident.

Data security breaches do not necessarily expose the consumer to ID theft or even to account fraud. In some instances, the breach may be the work of a hacker who had no criminal intent, or involve encrypted or incomplete information of no value to a criminal. Where the breach resulted in account fraud, protection of the consumer may require no more than account monitoring and the removal of unauthorized charges.

Nevertheless, some industry observers have suggested that credit card issuers should notify all customers and possibly reissue cards in every case in which any potential risk is found (even if the incident can not be verified or the consumers affected can not be validated). They also propose that consumers receive other assistance such as free credit report monitoring. These observers assume that the industry is resistant to such

[5] Account closure and the establishment replacement accounts is often unnecessary and entails costs that exceed the benefits. Where account closure is warranted, Discover facilitates the process. For example, preauthorized payment requests are automatically transferred to the new account so the customer does not have to contact the merchant or service provider and furnish the new account number.

requirements purely due to the cost involved. Given the fact that potential fraud-related losses are incurred by credit card issuers (not by consumers) and since actual fraud losses can quickly eclipse the cost of notification and/or card re-issuance, the cost of notification/re-issuance is generally not the driving factor for decisions about how best to react to a given situation.

Discover carefully weighs all relevant facts and impacts on our customers to determine the proper course of action (obviously complying with all relevant legal requirements). No purpose is served by notifying consumers who are not at actual risk of identity theft about data breaches if the consumer does not need to act to protect his or her information or avoid costs. Likewise there is no need to re-issue cards on accounts that have very low fraud risk. This provides no consumer benefit, but rather may cause inconvenience to consumers who have to activate their new cards and revise their numbers with all "recurring bills" (such as Internet, utility, and health care vendors) to avoid rejected transactions and potential lapse of service.

Of course, after-the fact notification, card re-issuance or other remedies do nothing to address the root cause of a given problem – identity theft. Prevention of data breaches and protection of information should be the primary focus of industry, regulators and the law.

Following the resolution of a data security incident, Discover's data breach Task Force reviews the situation and Discover's response to it to determine if changes are needed to

respond better to future incidents. The development of effective response initiatives is an evolutionary process due to changes in the threats we face. As criminals involved in identity theft become more sophisticated and nimble, we must respond accordingly.

CardSystems Solutions Data Breach

In response to the breach of credit card information held by CardSystems Solutions, we followed the procedures that I have described. The investigation of the incident is ongoing. But based on what we know today, it does not appear that Discover Cardmembers were exposed to a risk of identity theft as a result of CardSystem's loss of Discover data. And while the CardSystems breach *did* involve a loss of Discover data that could be used to commit account fraud, Discover Cardmembers will not experience financial loss as a result of this incident.

These conclusions are based on two facts. First, the Discover information involved in the CardSystems incident was limited to purchase transaction data. This information would not be useful to an identity thief in opening accounts with other financial institutions or otherwise taking over the identity of a Discover customer. Second, to the extent that the criminals involved in the CardSystems breach are able to use the information or make unauthorized transactions on some Discover accounts, our zero dollar fraud liability policy protects Cardmembers from financial loss. Our one-stop, 24/7, customer service program expedites the removal of unauthorized transactions from customer accounts.

Legislative Considerations

1. A national standard for responding to security breaches affecting personal financial information is appropriate. Criminals seeking access to consumer financial information rarely target residents of a single state: large-scale breaches potentially affect individuals across the country. Investigation, reporting, notification and remediation requirements that vary depending on the residence of an individual customer are more likely to impede than facilitate appropriate and prompt responses. National uniformity is needed. Legislation addressing security breach prevention or responses should preempt state laws addressing this subject.

2. For information held by financial institutions, we believe that the Interagency Guidance, coupled with on-site compliance examinations, establishes an effective and proper regime. It also provides regulators with the flexibility they need to adjust breach response standards over time as security threats evolve and the ability to prevent or react to them changes due to technological improvements and enhanced surveillance techniques.

3. Congress is considering proposed data protection and data breach legislation for unregulated entities that hold or process consumer financial information, but are not directly subject to statutory requirements. Coverage of such entities would be analogous to laws requiring merchants to protect customers (and payment card issuers) by suppressing or truncating credit card account numbers that are printed on sales receipts.

If Congress concludes that such broader security breach legislation is appropriate, the Interagency Guidance provides a good model for appropriate definitions, a consumer notice triggering mechanism, and response standards.

4. Finally, in the event of a data breach affecting credit card information, notification is best handled by the card issuer, not the entity whose security was breached. That entity whose security was compromised must cooperate fully in providing the details necessary to ensure efficient response and notification by the issuer, and to prevent further fraud. But requiring merchants or processors to directly notify affected cardholders may impose an obligation that they cannot readily achieve (since they may not have the necessary consumer contact information), and can needlessly alarm individuals who were not adversely affected by the breach. This might encourage consumers to take steps that are unnecessary (e.g., closing accounts, placing fraud alerts on credit reports). A single notice is the best way to protect credit card users, and card issuers are in the best position to determine whether and when that notice is appropriate.

Conclusion

Discover Financial Services appreciates the opportunity to discuss information security issues with the Subcommittee. We would be pleased to provide further information that would be useful to the Subcommittee in assessing the scope of the problem and the adequacy of current safeguards and response measures.