

Kevin Mitnick

Testimony Before the House Financial Services Committee

"Fighting Fraud: Improving Information Security"

April 3, 2003

Chairwoman Kelly, Chairman Bachus, and distinguished Members of the Committee –

My name is Kevin Mitnick. I appear before you today to discuss your efforts to review current industry practices concerning security procedures for the prevention of electronic theft of credit-card information. My understanding is that you are examining how to coordinate efforts among law enforcement, credit issuers, credit bureaus, and third-party vendors that process transactions, to limit harm to consumers and businesses when data security is breached.

I am primarily self-taught. My hobby as an adolescent consisted of studying methods, tactics, and strategies for circumventing computer security, and for learning more about how computer systems and telecommunication systems work.

I have 15 years experience circumventing information security measures, and can report that I have successfully compromised all systems that I targeted for unauthorized access, save one.

I also have two years experience as a private investigator, with responsibilities that included locating people and their assets using social engineering techniques.

I have gained unauthorized access to computer systems at some of the largest corporations on the planet, and have successfully penetrated some of the most resilient computer systems ever developed. I have used both technical and non-technical means to obtain the source code to various operating systems and telecommunications devices to study their vulnerabilities and their inner workings.

Currently I am the co-founder of Defensive Thinking, a Los Angeles-based information security firm. I recently co-authored with William Simon a book titled *The Art of Deception*, published by John Wiley and Sons, which has become an international bestseller. The book details non-technical methods and tactics – in essence, con-man techniques – that computer intruders use to compromise valuable information assets. The book also presents defensive techniques that companies and government agencies can employ to mitigate the risk of these so-called "social engineering" attacks.

Social engineering is a method where the intruder deceives his target into complying with a request based on false pretenses and psychological manipulation. It is important to understand – and all companies and their employees need to realize – that the most insidious vulnerability to information

security are the well-meaning, hard-working folks that use, operate, and maintain information systems.

The prevention and detection of social engineering attacks should not be ignored or underestimated. In fact, the majority of scams involving identity theft and credit fraud include social engineering on some level.

For instance, a thief can set up a phony ecommerce site by duplicating the real Web site of a Nike or a WalMart, and offer the products or services at what appear to be substantial discounts. The thief is then able to steer unsuspecting online shoppers to his phony site, where they enter their credit card numbers and other personal information to authenticate their purchases. The insider's term for stealing credit card information is "carding." After setting up his phony site, the "carder" then sits back and collects the credit-card information that pours in.

Another method that credit card thieves use to obtain private financial information is to send a phony instant message or forged email message that purports to be from the target's Internet Service Provider or an eCommerce site. The message explains that some kind of problem has occurred, and requests the user to provide his or her login name and password, or to reveal financial information.

In an attempt to deter carding, many retailers are now requiring an online customer to provide the three-digit CVC number that card issuers have begun to use. But the thief also asks for this CVC number. With it, he is able to use the information to commit fraud against an unsuspecting cardholder and the merchants.

In my previous testimony before the Committee on Governmental Affairs in March of 2000, I detailed the common vulnerabilities exploited to gain unauthorized access to information assets or computing resources. I recommended several risk mitigation strategies to increase the effectiveness of future security and reliability of information systems owned and operated by, or on behalf of, the federal government.

At the time, my testimony focused on the vulnerabilities of Federal computer systems – but these same vulnerabilities also exist throughout the private sector.

As you probably already know, identity theft and credit-card fraud are the fastest growing crimes of the decade.

I understand that the subcommittee will be examining three recent cases involving large-scale thefts of non-public personal identifying information and credit card details. A major part of the problem is that the criminals only needed to obtain information that is stored or processed in thousands of computer systems. You will learn that the methods they used varied from low-tech skimming of cards by unscrupulous employees, to circumventing complex security measures at sites that store or process credit card information.

In February, 2003, DPI, a credit card processing services company, reported that an unknown intruder had compromised their network and gained access to a

database that held over eight million credit card accounts. DPI did not release any details describing how the breach occurred, citing cooperation with Federal law enforcement officials.

The DPI case was widely reported in the press because of the astounding number of credit cards potentially compromised. But when examined closer, you will realize that these types of attacks happen all the time.

Subsequent to the DPI incident, computer intruders compromised a Georgia Tech computer system and obtained access to 57,000 credit card numbers.

In my opinion the committee should not overlook that many similar attacks on networks containing financial information are not detected by the owner or operator. It is important to realize that many of these security incidents remain undetected because of poor security and auditing practices.

DPI has publicly claimed that the intrusion occurred from outside the organization. Although I don't like to hypothesize on facts and circumstances of any attack without details, I would recommend that DPI consider the possibility that the attacker had assistance from the inside of the company.

Based on my experience, I would say that the attackers were able to exploit a technical vulnerability in the operating system or a particular service that was available to attacker via the Internet.

Every day the security community announces new vulnerabilities in operating systems and application software that have just been identified. Vulnerabilities in software can be exploited to gain remote access to the target computer. Many system programs contain programming errors that enable the intruder to trick the software into behaving in a way other than that which is intended in order to gain unauthorized access rights, even when the application is a part of the operating system of the computer.

Once a new vulnerability is recognized, the software developer or a security company develops a "patch" – a modification to the software – that must then be installed by individual companies, a process that may be overlooked for days, weeks, or even months. Meanwhile companies using that software remain vulnerable, or are forced to disable or block access to the vulnerable service until the patch becomes available.

Even then, in many cases, this is not enough. There are any number of sophisticated hackers who are able to discover previously unrecognized security vulnerabilities, and then use them to compromise computer systems and networks.

As a point of information – the programming instructions to exploit a new vulnerability may be well known to hackers, but the software manufacturer has not been notified of the problem.

This type of crime will continue to be attractive to electronic criminals as long as credit-card details are stored by businesses connected to the Internet.

I agree that it is essential to implement security strategies to prevent, detect, and respond to security threats and attacks. But it's too easy to look in the wrong direction for an answer. In my view, attempting to solve the complex problem by micro-managing every online site that accepts credit card transactions would turn out to be a wasteful, inefficient, and not a very successful exercise.

Instead, I recommend that the committee look in a different direction. I recommend that you explore mitigation strategies which focus on improving the authentication of the credit card user.

The challenge is a good deal easier when the customer is standing in a brick-and-mortar retail outlet with his or her credit card in hand. In this kind of face-to-face situation, mitigating fraudulent transactions may be achieved by assigning every credit card holder a personal identification code -one that is not printed on the credit card itself. This provides a two-factor form of authentication that is harder to circumvent as compared to merely depending on the possession of the physical card.

But this solution would not eliminate problems with online transactions, the situation that the credit-card industry refers to by the curious term "Card Not Present" –meaning that the cardholder is not face-to-face with a retail clerk or the like. In any online credit-card transaction, identity and authorization is based on the information a consumer provides to the merchant. This is no better than a static password. There's an old saying among hackers: "You never know if someone else has your password." The reality is that a password or its equivalent is too easy to steal.

A first step toward a solution would be to strip away the identity value of all personal information. If knowledge of a credit card number, expiration date, and the corresponding customer name and address is without value, stealing this information would be useless to an imposter. Unfortunately, authentication technology has not yet matured to the point of being able to provide a solution to this issue.

But the process of requiring another authentication factor would add cost to the entire infrastructure of business and would result in loss of sales due to consumer inconvenience. If not being done already, I would recommend that the industry explore using additional authentication practices that may include digital certificates; identification of the user's location based on IP address or telephone number; or verification of a PIN through another communication channel. For example, consider this scenario: You've just placed an Internet order for a new cell phone with a price tag of several hundred dollars, and placed an online order with your credit card information. But you were not required to give a PIN number. Instead, you next dial your credit-card company, and when prompted, enter your card number. An automated system then reads off details of the transaction. You are satisfied that the details are correct. The system then tells you, "To authorize this transaction, enter your PIN number."

This process would probably be used only for more expensive Internet purchases, since it does require an extra step by the consumer and additional cost to the credit-card companies for handling the authorization phone calls.

What would be the advantage of this approach? The thousands upon thousands of individual retailers would not have access to consumer PIN numbers. The fact that so many retailers store the credit-card numbers of online customers gives rise to the kind of card-number theft that this hearing is addressing. If they also store the customer's PINS, then there's no gain in security – the PIN becomes almost worthless as a security element.

But under the approach I've suggested, only the card issuer would have access to the PIN-number information. Under this arrangement, theft of the card numbers would be of limited value. Using a card for many fifty-dollar purchases makes the bad-guy more susceptible to identification and arrest.

In another area, I also recommend consumer awareness training programs that educate people about the various scams being used to steal their credit card details and personal information, a practice that can prove highly valuable to effectively minimize identity theft and credit card fraud.

So I respectfully submit for your consideration these recommendations for the improved security of online retail transactions and credit-card protection against theft and fraud. I believe that all online retailers who accept credit card should be encouraged or required to do the following –

- 1) Perform a regular, thorough risk assessment of their information assets, especially systems that process or store consumer financial and personal information.
- 2) Implement policies, procedures, standards and guidelines as dictated by the results of the risk assessment.
- 3) Create an audit and oversight program that measures compliance. The frequency of the audits ought to be determined consistent with the mission; the more valuable the data, the more frequent the audit process.
- 4) Develop a process to insure meaningful and effective patch and configuration management for all computer systems.
- 5) Employ authentication methods that do not use non-public personal identification information such as mother's maiden name, birth date, birth place, driver's license number, address, phone number, or social security number.
- 6) Effective audit procedures – implemented from the top down – must be part of an appropriate system of rewards and consequences in order to motivate system administrators, personnel managers, and employees to maintain effective information security consistent with the goals of this committee.
- 7) Establish a security awareness training program designed to educate their employees on threats to information security, and to change employee behavior to foster a secure environment. These would follow security recommendations described in detail in my book *The Art of Deception*.

In terms of legislation, I recommend that the subcommittee consider the following:

- 1) Legislation that prohibits merchants or credit card processors from electronically storing PINS or other types of verification credentials such as CVC and CVC2, unless essential to business needs.
- 2) The requiring of periodic security assessments/penetration testing to evaluate the security posture of any business that stores or processes credit card transactions, to be performed by an independent information security consulting firm.

Finally, I want to offer what I have deemed to be the most important factor in security: the human factor. This is the essential, underlying all security issues, whether it's from deceptive credit card thieves or terrorist operatives that blend into our communities. This nation needs to train the community at large to recognize the deceptive tactics used by credit card and identity thieves to dupe into revealing their information, while still allowing individuals to retain the qualities of kindness and humanity that characterize the American people. I believe we as a people need not give up the qualities of trust and truth in order to gain strength against being duped and damaged. Training, training, training – and I believe it's essential to consider regulations that mandate security awareness training as part of an overall security program as required by HIPAA and GLBA. .

Now I will gladly answer any questions the members of the subcommittee would like to ask me.