Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Skimming and Its Side Effects

Skimming is a topic that I had never heard of until a work associate, whom was making suggestions for my practical, mentioned it. I was quite curious and embarked to see whether I could find any information on this topic. My associate did not know the term used for this activity or that for the device used to accomplish it. However, upon speaking to my mentor about it, he provided the appropriate term, "skimming," and indicated that this might be a good topic. What I have learned in my research has truly amazed me and ...

Copyright SANS Institute
Author Retains Full Rights

AD

# Skimming and Its Side Effects

Nobie Cleaver

Practical Assignment, Version 1.4b

November 20, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

TABLE OF CONTENTS

Abstract

What is skimming?

What is a skimming device?

Types of skimming devices:
- Those that cause ATM malfunctions
- Those that do not cause ATM malfunctions

How is it done?

Statistics

Liability

Solutions and recommendations

How to avoid being skimmed

If you become a victim of skimming

Identity Theft

How to protect your identity

How to know if your identity has been stolen

What to do if your identity has been stolen

The Identity Theft and Deterrence Act of 1998

Other federal laws related to identity theft

- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act
- Electronic Funds Transfer Act
- Fair Credit Billing Act
- Fair Debt Collection Practices Act

© SANS Institute 2004, Author retains full rights.

Abstract
Skimming is a topic that I had never heard of until a work associate, whom was making suggestions for my practical, mentioned it. I was quite curious and embarked to see whether I could find any information on this topic. My associate did not know the term used for this activity or that for the device used to accomplish it. However, upon speaking to my mentor about it, he provided the appropriate term, "skimming," and indicated that this might be a good topic. What I have learned in my research has truly amazed me and I endeavor to share some of that information in this paper.

I will define skimming, describe what a skimming device may look like, discuss how skimming is done, provide some statistical information and provide some pointers on how to avoid being skimmed and what to do if it happens. In addition, I will provide some of the industry solutions and recommendations for this international problem. For those who have had their card information stolen and/or had their identities stolen as a result of skimming, I will provide information that may be helpful to your recovery.

What Is Skimming?
Skimming is a process whereby the account information that is electronically stored on the magnetic stripe of a credit card or debit card is illegally copied during an attempt to use an automatic teller machine (ATM). The personal identification number (PIN) information is also illegally attained in conjunction with the card skimming. Then the account information is used to produce counterfeit cards and used with the stolen PIN to withdraw cash or to make unauthorized purchases.[1]

What is a skimming device?
A small, inexpensive, electronic device, about the size of a pager,[2] [3]

Types of skimming devices:
*Those that cause the ATM to malfunction*: The skimming device is inserted into the slot of the ATM machine where the credit card would normally be swiped. When the consumer inserts or swipes his card, it is not read by the actual ATM, but rather, by the illegitimate skimming device. Consequently, the consumer's intended transaction does not occur. This can be a hint to the cardholder that the machine may have been tampered with.[4].

---

[1] Schmidt, Lucinda. " Warning signs." 15 Oct. 2003. URL: http://moneymanager.smh.com.au/articles/2003/10/15/1065917445606.html (14 Nov. 2003).

[2] "skimming is a scam." URL: HTTP://usa.visa.com/media/business/skim2.pdf (14 Nov. 2003).
[3] Milner, George with Sam Ott, Michele Petry and Mary Beth Guard "Skimming, Scanning, and Scamming: ATM Crime On The Rise
." 16 May 2003. URL: http://www.bankersonline.com/security/gm_atm_skimming.html (16 Nov. 2003).
[4] " Wisconsin Bankers Association Warns Consumers, Asks for Help In Identifying ATM Card Skimming Scam." 7 May 2003. URL: http://www.wisbank.com/Media/Press%20Releases/PR_ATM_Card_Skimming_Scam.htm (14 Nov. 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

*Those that do not cause the ATM to malfunction*: This type of skimmer "is placed over the card reader but doesn't block off the reader."[5] It may be "attached with double sided tape" and stick out half an inch from the ATM.[6] In this instance, the consumer's intended transaction does occur. This scenario, seems more troubling to me since the crime not may be realized until the consumer receives his monthly statement and notices purchases he did not make.

How is it done?

In a very sophisticated operation, a skimming device made from metal similar to that of the real ATM is designed to fit onto the machine; an attached laptop is concealed inside. In this setup, a touch-screen is used to prompt the customer. The keypad is not used, but the card reader is. Signage indicating a change in the normal operation of the ATM has been posted. The customer swipes his card (the data being recorded by the computer) and receives a "Welcome" screen and instructions, just as he normally would. During the process, the PIN number is also saved onto the laptop. Before the transaction is completed, the ATM user receives an error message that the machine has malfunctioned.[7] In this instance, all the account data necessary to produce and use a counterfeited duplicate card is stolen in one smooth process. However, the customer not only becomes the victim of fraud, but also fails to complete his intended transaction.

In a similar, but subtler operation, a transparent skimming device is placed inside the card reader slot. A computer is also used in this scam and a transparent plastic overlay embedded with microchips is placed over the ATM keypad. As in the previous example, both the stripe data and PIN is captured and copied without any suspicion by the cardholder since there is no interference with the normal transaction.[8]

In a simpler scenario, a portable skimming device that also prevents the machine from functioning properly is attached to the ATM. However, in this case, the con person is there to pretend to assist the ATM customers with their transactions. It is through this purported assistance that the con person acquires the PINs.

In a different skimming scam, the prospective thief installs onto the ATM machine a skimming device that may not be distinguishable from the regular card reader. This device does not interfere with the normal operation of the machine, but the skimming device copies the stripe data. The PIN information is captured by a small video camera positioned to view the keypad. The thief later retrieves both the skimming device and the camera. It is common for this type operation to be

[5] Schmidt, Lucinda. " Warning signs."
[6] " Wisconsin Bankers Association Warns Consumers, Asks for Help In Identifying ATM Card Skimming Scam."
[7] Bruce, Laura. "Skimming the cash out of your account." 24 Mar 2003 URL: http://www.bankrate.com/brm/news/atm/20021004a.asp?prodtype=bank (14 Nov. 2003).
[8] "New reasons to guard your ATM card." URL: http://moneycentral.msn.com/content/Banking/P57803.asp?Printer (14 Nov. 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

performed during a time of high-volume ATM transactions.[9] A variation of this scam occurs when the thief is actually present to look over the cardholder's shoulder (referred to as "shoulder surfing"[10]) or otherwise scrutinize the input of the PIN number.

In all cases, it is easiest to attach skimming devices to ATMs with raised card readers, also referred to as "swipe readers"[11]

In another scenario, the skimming activity occurs at a place, like a restaurant or a gas station that allows its customers to make purchases with credit or debit cards. This is referred to as a point of sale (POS) transactions. Either of two things may happen: The merchant's attendant may double swipe the card, i.e., slide it through the official POS reader and also through a skimming device. Or the POS reader may be attached to a hidden laptop that has been configured so that it will copy the card's stripe data as it is being read. In both cases, a video camera may be hidden to record the customers entering their PINs or a keystroke-recording device may have been attached to the POS machine.[12] The stolen stripe data is encoded onto blank cards to produce illegal duplicates of the official cards.[13] These may be used or sold, along with the PIN numbers, on the black market.

In any of these examples, a tiny camera may be been placed on the actual keypad to record the PIN as it is being entered.[14] Or the perpetrator may use binoculars to watch the customer. Another way PIN numbers may be acquired is through telephone or email scams. The thief, posing as someone from the consumer's financial institution, will call or email consumers and try to trick them into releasing their PIN numbers.[15]

In all of these examples, the information obtained from a skimming scheme may be used in what is known as card-not-present transactions. "This type of fraud

---

[9] D'Angelo, Frank and Stephanie Cook." ATMs: Offering Convenience to Customers and Opportunities to Criminals." Aug./Sep. 2003 URL: http://www.wib.org/wb_articles/fraud_aug03/ATMs_aug03.htm (14 Nov. 2003).
[10] Aminu, Ayodele. "Association Raises Alarm Over ATM Fraud." 25 July 2003 URL: http://www.thisdayonline.com/archive/2003/02/05/20030205bus01.html (14 Nov. 2003).
[11] " Beware of ATM Scams." St Cloud Federal Credit Union. Jan 2003. URL: http://www.stcloudfcu.com/newletter/2003_jan.pdf (14 Nov. 2003).
[12] "Financial Fraud: Important Lessons for Young Consumers." Money Matter$, Fall 2003. URL: http://www.gettingfiscallyfit.org/highschool/fall03.pdf (16 Nov. 2003).
[13] "What You Need To Know About Card Skimming ."
[14] Tatum, Christine. "'Skimming' milks ATM customers cash ." 1 May 2003. URL: http://www.chicagotribune.com/technology/local/profiles/chi-030501downloads,0,802804.column?coll=chi-shopping-hed (14 Nov. 2003).
[15] "Financial Fraud: Important Lessons for Young Consumers."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

occurs when neither the card nor its owner is present at the point-of-sale."[16]The account data is used to make Internet, telephone and mail order purchases.[17]

Statistics

Skimming started in the late 1990's, but has become easier to accomplish with the development of smaller computer components.[18]

In the United States alone, there are approximately 365,000 ATM machines,[19] generating greater than 41,000,000 transactions daily.[20]; Fifty percent of the ATMs are owned by banks and fifty percent by other merchants that place their ATMs in establishments such as restaurants, hotels, shopping malls, convenience stores, airports, etc.[21] Each of these is a potential target for prospective criminals or crime rings

Skimming can involve the transfer of huge sums of money. According to the American Bankers Association, $51 million was lost due to debit card fraud.[22] In a New York crime ring, about $3.5 million was stolen before the criminals were apprehended. This case involved greater than 20 ATM machines, thousands of ATM cards, 1,400 cards issuers, and in excess of 26,000 ATM transactions.[23]

"Most ATM activity occurs during the evening"[24] and the thieves rarely stay in the same area for more than seven to ten days.[25] The "counterfeit cards (are) produced within 24 hours" [26] and fraudulent transactions are performed within 24 to 48 hours after the swipe data and PIN are stolen.[27]

Other skimming cases in the United States have been reported in – Boca Raton, Florida, Illinois, Kansas, Maryland, Virginia, Wisconsin, South Carolina, and Colorado, as well.[28] [29]

---

[16] "Card Fraud The Facts 2003." URL: http://www.cardwatch.org.uk/pdf_files/cardfraudfacts2003.pdf (14 Nov. 2003).
[17] "Card Fraud The Facts 2003."
[18] Bruce, Laura. "Skimming the cash out of your account."
[19] Tatum, Christine. "'Skimming' milks ATM customers cash ."
[20] "Beware Scams At Your ATM."
[21] Bruce, Laura. "Skimming the cash out of your account."
[22] "New reasons to guard your ATM card."
[23] Bruce, Laura. "Skimming the cash out of your account."
[24] Milner, George with Sam Ott, Michele Petry and Mary Beth Guard "Skimming, Scanning, and Scamming: ATM Crime On The Rise."
[25] Annese, John."Customers reimbursed ." 12 Aug. 2003 URL: http://www.zwire.com/site/news.cfm?newsid=10001183&BRD=985&PAG=461&dept_id=161556&rfi=6 (14 Nov. 2003).
[26] D'Angelo, Frank and Stephanie Cook." ATMs: Offering Convenience to Customers and Opportunities to Criminals."
[27] D'Angelo, Frank and Stephanie Cook." ATMs: Offering Convenience to Customers and Opportunities to Criminals."
[28] Tatum, Christine. "'Skimming' milks ATM customers cash ."
[29] [29] Milner, George with Sam Ott, Michele Petry and Mary Beth Guard "

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

But skimming is not just of national concern, it is also an international problem. Cases have been reported in Australia, South Africa, France, Spain and many other parts of the world.[30] [31] [32] The Australian Crime Commission estimates that skimming is responsible for $300 million a year in that country and that much of this crime is being committed by organized crime rings linked with Malaysia. Indonesia, Hong Kong and Thailand.[33] And Ian McKindley, Head of Fraud Control with Visa International, reports that in the last year, skimming increased by 300 percent.[34]

Liability

ATM crime costs the industry millions of dollars a year, but, fortunately, the consumer does not bear most of the liability.

The Bank of America spokesperson, Lisa Gagnon, reported that "Bank of America protects its customers against fraud in many ways, which includes our commitment to assume 100 percent responsibility for the cost of the fraud for customers who have unauthorized activity on their ATM or check card."[35]
On the other hand, under Federal Reserve regulations, you are liable for a maximum of fifty dollars if you report, within two business days, that your ATM or debit card was lost or stolen.[36] Otherwise, you may be liable for up to five-hundred dollars.[37]

Similarly, the Truth in Lending Act (TILA) states that the cardholder is only liable for charges of up to fifty dollars once he reports the unauthorized purchases.[38]

Solutions and recommendations

A special task force, has been created by the Electronic Funds Transfer Association (EFTA), which is "committed to the advancement of the electronic payment systems and commerce industry"[39] to address the problem of skimming.[40] This task force is headed by Kurt Helwig, the director of the EFTA, and includes members from the United States Secret Service and all segments of the ATM industry [41]

---

[30] Milner, George with Sam Ott, Michele Petry and Mary Beth Guard "Skimming, Scanning, and Scamming: ATM Crime On The Rise."
[31] Aminu, Ayodele. "Association Raises Alarm Over ATM Fraud."
[32] "Card Fraud The Facts 2003."
[33] " Card Skimming "Booming Cybercrime." URL: http://www.asianlaws.org/infosec/archives/07_03_card.htm (14 Nov. 2003).
[34] "AVOIDING CREDIT CARD FRAUD." family WATCH. Jan. 2003. Issue No. 16. URL: http://www.ccinsurances.com.au/publications/family_watch_issue_16.pdf (14 Nov. 2003).
[35] Bruce, Laura. "Skimming the cash out of your account."
[36] "New reasons to guard your ATM card."
[37] "Financial Fraud: Important Lessons for Young Consumers." Money Matter$, Fall 2003. URL: http://www.gettingfiscallyfit.org/highschool/fall03.pdf (16 Nov. 2003).
[38] "Financial Fraud: Important Lessons for Young Consumers."
[39] Shaping the Future of the Electronic Payments and Commerce Industry"
[40] Tatum, Christine. "'Skimming' milks ATM customers cash ."
[41] Bruce, Laura. "Skimming the cash out of your account." 2

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

In May 2003, the EFTA's ATM integrity task force released its first report. The main points of "Issue 1: Recommendations to Manufacturers for Improving PIN Security within the ATM" are copied below:[42]

- The existing standards for key management and PIN security should remain the standard to which ATMs should adhere with respect to encryption and key management. In the U.S., these standards are the ANSI X9.24 for Key Management and ANSI X9.8 for PIN encryption.
- All of the major manufacturers should form a representative group of manufacturers to:

  - Develop a common interpretation of these standards. (All ATMs should follow the industry encryption standards from the point of initial PIN entry and through the entire system.)
  - Collectively present a request to Underwriters Laboratory ("UL") and other independent testing authorities to modify the existing UL291 standard for ATMs so as to include a certification that the UL approved model meets the standards as interpreted.

    Future UL291 listings would, therefore, include interpretation of the standards, and all manufacturers seeking such listings would be evaluated against this common standard by an independent third party.

- Manufacturers should communicate that all current and future equipment manufactured by them meets the ANSI X9.8 and ANSI X9.24 standards (and other international standards applicable in each country) as clarified with respect to:

  - The point at which the PIN is entered into the system (i.e., the external surface of the keyboard);
  - The point at which the PIN is encrypted for transmission;
  - The path between the above-noted two (2) points.

  It should be noted that current production models of many, if not all, major manufacturers are believed to have encrypting PIN Pads consistent with this recommended interpretation.

- Manufacturers, if they have not already done so, should identify:

[42] "ARM INTEGRITY TASK FORCE RECOMMENDATIONS ON BEST PRACTICES." 30 May 2003 URL: http://www.efta.org/new/FINAL_Report.pdf (16 Nov. 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Legacy machines, by model description, that will be able to be upgraded to the above-defined standards;
- The upgrade path (i.e., replacement kits, software upgrades, etc.) available for these upgradeable legacy machines;
- Those legacy machines that do not and will not have upgrade paths available to them.
- The schedule for compliance of legacy machines that can be upgraded through use of upgrades/retrofit kits should enable these upgrades to occur in conjunction with other previously established timetables for upgrades to comply with DES 3 and other mandates, so as to maximize efficiency and minimize costs associated with such upgrades of the installed ATM base.

Additionally, as an ongoing responsibility, the United States Secret Service investigates ATM crime and makes recommendations. They have warned financial institutions to be aware of "any foreign device in or around the ATM, including card readers, overlays, and cameras."[43]

Some companies are building new ATM machines with the card "reader embedded deep within the machine."[44] This is being done in an effort to make it harder for the prospective criminal to attach a skimming device to the ATM. Others are installing alarms that indicate when the card reader on the ATM becomes blocked.[45]

Another technology used to deter skimming is referred to as jitter. Jitter causes the speed at which the card is moved through the reader to be vary so that the process is not smooth, which is necessary for many skimmers to work. The card is also forced to move back and forth during the process of being read.[46]

At the March 2003 MasterCard International symposium, MagTek Inc introduced its technology to help prevent skimming. Called the Magneprint solution, it uses "the intrinsic noise" properties of the magnetic stripe, unique for every card, to differentiate between the original and a cloned card."[47] Magneprint has been successfully beta tested in Malaysia.[48]

---

[43] D'Angelo, Frank and Stephanie Cook." ATMs: Offering Convenience to Customers and Opportunities to Criminals."
[44] Milner, George with Sam Ott, Michele Petry and Mary Beth Guard "Skimming, Scanning, and Scamming: ATM Crime On The Rise."
[45] Aminu, Ayodele. "Association Raises Alarm Over ATM Fraud."
[46] Milner, George with Sam Ott, Michele Petry and Mary Beth Guard "Skimming, Scanning, and Scamming: ATM Crime On The Rise."
[47] Costa, Christina. "MasterCard International Hosts First Global Risk Management Symposium." 13 May 2003. URL: http://www.mastercardintl.com/cgi-bin/newsroom.cgi?id=706 (16 Nov. 2003).
[48] Costa, Christina. "MasterCard International Hosts First Global Risk Management Symposium."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The UK uses the "Chip and PIN system."[49] The objectives of this system are to ensure that the card being read is genuine, and that the person using it is the true owner. This method replaces the magnetic stripe and signature system. To ensure that a card is not a counterfeit, the microchip on the card keeps the information secure, thus, preventing skimming. In 2002, more than 41 million chip cards were in use in the UK, nearly half a million chip terminals were deployed, and more than 25,000 chip readers were installed in cash machines. „[50]

To fulfill the objective of validating the real card owner, by 2005, reports the Association for Payment Clearing Services (APACS), most credit and debit transactions made in person in the UK will be authorized by PIN instead of signature. Furthermore, they predict that also "by 2005 all of the UK's credit and debit cards will be reissued with chip and PIN capability.[51]„
The UK will be one of the first to implement this technology on a nationwide scale. And "all European countries are already preparing their migration, and most other parts of the world are expected to follow suit over the next three to four years."[52]

Since these technologies are only being installed in new ATM machines, they do not address the risk of skimming that still exists with the currently installed base of machines.

One way financial institutions are trying to combat this is by using special software programs that allow them to identify unusual spending patterns or "geographical anomalies"[53]. When an incident is noticed, the cardholder is contacted, possibly before he receives a statement or becomes aware of any unauthorized purchases, to confirm whether the transactions are valid.[54] In the case of fraud, the card is inactivated.

In some places, merchants impose a limit on how much the card customer may purchase before requiring the card issuer to authorize. Other institutions utilize databases of lost or stolen cards and use them to check card transactions for matches. In an effort to prevent thief, some banks use special delivery services to distribute new cards to their customers.[55]

To help prevent card-not-present crime, a system has been developed to enable the cardholder to verify his billing address and card security code. For these transactions, the user is asked to provide the complete address and the "last

[49] "Card Fraud The Facts 2003."

[50] "Card Fraud The Facts 2003."
[51] "Card Fraud The Facts 2003."
[52] "Card Fraud The Facts 2003."
[53] "New reasons to guard your ATM card."
[54] Schmidt, Lucinda. " Warning signs." 1
[55] "Card Fraud The Facts 2003."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

three or four-digit number" that is printed below the signature panel on the card. This is the security card.[56] This request for additional information helps to minimize the risk of fraudulent transactions.

How to avoid being skimmed [57] [58] [59] [60] [61] [62] [63]

Only use an ATM during the day.
Choose an ATM in a high traffic, public place where there is good lighting and nothing that may obstruct a waiting thief from view.
Do not use an ATM where an unusual sign is posted.
Be alert at ATMs. Do not accept assistance from anyone. If anyone interrupts when you are at the ATM, cancel your transaction and retrieve your card.
If you notice anyone loitering or taking pictures near the ATM, do not use it, choose another location.
Become familiar with the appearance of a legitimate ATM. Observe the ATM before using it. If the card reader is discolored, anything is stuck to the ATM, the machine does not otherwise look normal or the keypad does network, do not use it.
After using an ATM, if your card is not returned, report this to your financial institution, immediately.
Never record your PIN or carry it in your wallet or purse. It's best to put this number to memory.
Do not select an obvious PIN, such as your birth date or social security number.
Do not provide your card number on the telephone to anyone with whom you did not initiate the call, and do not ever verbally state the number in the presence of anyone near enough to hear you.
Never reveal your PIN to anyone, in person or on the telephone. Know that your bank will not call and ask you for this information
If the ATM monitor does not prompt you for your PIN, do not enter it. Report the malfunctioning machine to your financial institution.
When entering your PIN, position yourself as close as possible to the ATM and cover the keypad with your free hand, or in some other way try to conceal the keypad.
For POS transactions, never let your card out of your site.
*For Internet transactions*:[64]
Be sure your browser is configured for maximum security.

---

[56] "Card Fraud The Facts 2003."
[57] "What You Need To Know About Card Skimming ."
[58] " Wisconsin Bankers Association Warns Consumers, Asks for Help In Identifying ATM Card Skimming Scam."
[59] Milner, George with Sam Ott, Michele Petry and Mary Beth Guard "Skimming, Scanning, and Scamming: ATM Crime On The Rise."
[60] Bruce, Laura. "Skimming the cash out of your account."
[61] "Card Fraud The Facts 2003."
[62] " How to be ATM "Streetwise"." URL: http://nsi.org/Tips/atmtips.html (16 Nov. 2003).
[63] Costa, Christina. "MasterCard International Hosts First Global Risk Management Symposium."
[64] "Card Fraud The Facts 2003."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Look for the locked padlock or unbroken key symbol in the bottom right hand of your browser window. This is the security icon. Be sure you see this before transmitting your card data and that the "http" in the web address has changed to "https" to indicate that your connection is secure.
To confirm that the date of the encryption certificate has not expired and that the vendor's certificate shows the same address as that in the address bar or location bar of your browser, click the security icon and check these items.
Reserve one of your credit cards for Internet use only if you are a regular online shopper.
Shred transaction receipts before discarding.

<u>If you become a victim of skimming</u>
Report it to your financial institution immediately.
Stop using the card.
If unauthorized transactions have been made, notate these on your statement and provide that information to the financial institution.

<u>Identity Theft</u>
that
If having your debit or credit card "skimmed"is not bad enough, getting your identity stolen as a result of this criminal activity is much worst. In fact it can be devastating.

Identity theft has become widespread and can be costly and long lasting. Moreover, the data stolen via skimming can lend to building up a profile of information that can be useful in the creation of counterfeited documents needed to create a false identity.

Simply put, identity theft occurs when a person steals someone else's personal information and uses it to commit a crime (such as opening up a credit account) without the victim's knowledge. Identity theft may also be referred to as "ID Theft, Identity Fraud, Bank Fraud, Account Takeover, Credit Card Fraud, Criminal Identity Theft, Check Fraud, New Account Fraud, or Wire Fraud."[65]

Identity theft can be accomplished in at least a couple of different ways. In *application fraud*, bank statements, and other stolen or false documents are used to apply for accounts in the victim's name.[66] For example, this identity thief may open up a bank account or credit card account, take out a loan or acquire telephone and utility services, apply for social services, rent an apartment, buy a car, take out mortgage, etc.[67] [68]

---

[65] "What is identity theft?"
[66] "What is identity theft?"
[67] "PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON IDENTITY THEFT. " 13 Sep. 2000. URL: http://www.ftc.gov/os/2000/09/idthefttest.htm (16 Nov. 2003).
[68] "What is identity theft?"

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

In an *account takeover*, the criminal pretends to be another person (who becomes the victim) by using personally identifying data that was taken from stolen documents or media (such as that stored on the magnetic strip of an ATM card) and contacts the appropriate institution (the credit card issuer, for instance) to have the billing address changed. Then the thief reports the card as lost and requests that a replacement is mailed to the new address.[69]

Other examples of identity thief include writing fraudulent checks in the victim's name and/or using the victim's account number, and completely taking over another person's identity.

How to protect your identity[70] [71]

Store personal data in a safe place. Always safeguard your wallet or purse.
Do not keep essential documents, such as your Social Security card, birth certificate, visa or passport, in your wallet or purse.
Provide personal data only when absolutely necessary and only to trusted individuals.
Before discarding card receipts or other documents containing personal data, shred them.
Know when to expect your monthly financial statements and review them regularly. Report any discrepancies found, or if any of them is missing.
Provide your new address to your financial institution if you move.
Never record your credit or debit card number on other documents, such as checks, for the purpose of identification.
Never provide personal identification information to anyone over the telephone unless it is essential and you trust the person.
Keep a list of all your financial accounts along with the institutions' telephone numbers in a safe place. This will be very useful if your cards are lost or stolen.
Request and review your credit report on an annual basis. Report to the credit bureau any discrepancies found immediately. Keep copies of all correspondence. Sending by registered mail gives you the option of requesting delivery confirmation.

How to know if your identity has been stolen[72]

You fail to receive monthly statements from your financial institution and other expected mail.
Your card statements contain unauthorized transactions.
You start to receive calls from debt collection agencies for purchases you did not make.
You receive calls regarding approved or denied credit cards that you did not apply for.

---

[69] "Card Fraud The Facts 2003."
[70] "Card Fraud The Facts 2003."
[71] Costa, Christina. "MasterCard International Hosts First Global Risk Management Symposium."
[72] "Card Fraud The Facts 2003."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

What to do if your identity has been stolen[73] [74] [75]

Since it is impossible to guarantee that your identity will not be stolen, it is wise to know, in advance, what to do if it happens. The following steps should be helpful:

Immediately, report the incident to the customer services department of the financial institution for the account involved. Verify that your billing address is correct. Your card will probably be canceled and a replacement issued.

Report the incident to one of the credit bureaus listed below. (Always follow-up any telephone conversation with correspondence.) That agency will contact the other two. Additionally, an automatic fraud alert will be placed on your credit report within 24 hours at each of the bureaus. The purpose of the fraud alert is to prevent your creditor from authorizing additional credit to the identity thief.[76]

Equifax
(800)-525-6285
P.O. Box 740241,
Atlanta, GA 30374-0241

Experian
(888)-397-3742
P.O. Box 949,
Allen TX 75013-0949

Trans Union
(800)-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834

Contact the appropriate agencies, such as the Federal Trade Commission (1-877-438-4338), Social Security Administration and your local police department

Review your future monthly financial statement(s) to verify that your account has been correct

Change the passwords on all of your accounts. Do not make easily guessed choices such as your mother's maiden name or the last four digits of your Social Security number for your PIN.

If the identity thief has used your driver's license number, request a new one from the Department of Motor Vehicles.

---

[73] Costa, Christina. "MasterCard International Hosts First Global Risk Management Symposium."
[74] Lazarony, Lucy. Identity theft serves up double threat to victims." 28 Apr. 2003. URL:http://www.bankrate.com/brm/news/pf/20010226a.asp (20 Nov. 2003).
[75] "What to do if you identity is stolen."25 Apr. 2003. URL: http://www.bankrate.com/brm/news/pf/20010301a.asp (14 Nov. 2003)
[76] Lazarony, Lucy. Identity theft serves up double threat to victims."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Make your utility and telephone companies aware of the identity theif incident in case the imposter tries to use the addresses on these accounts to prove residency.
This process may take weeks, months or years. So be patient, but persistent, because the burden of proof does rest on you, the victim. One bit of good news is that you will only have to complete one fraud declaration report, which has been standardized by the Federal Trade Commission. Then you can file a signed copy with each financial institution.[77]

The Identity Theft and Assumption Deterrence Act of 1998
This act is also known as the "Identity Theft Act." It establishes the Federal Trade Commission as the agency to be the national clearinghouse for identity theft complaints, victim assistance and consumer education. The Identity Theft Act amends Title 18 U.S.C. 1028 to make identity theft a federal crime that is punishable by a fine of up to $250,000 and or imprisonment of not more than fifteen years.[78] It also focuses on the consumer as the real victim of identity theft and authorizes the Commission to refer complaints to the three major national consumer-reporting agencies.[79]

In the Commission's plan to meet its responsibilities, it has implemented a toll-free telephone hotline for consumers to use to report identity theft and a complaint database, referred to as the Identity Theft Data Clearinghouse, which is available to law enforcement agencies nationwide. It also coordinates with other government agencies and organizations to develop and distribute educational information about identity theft.[80]

Other federal laws related to identity theft
*Gramm-Leach-Bliley Act* (GLB Act): This act prohibits "pretexting" which is the attempt to fraudulently obtain customer information from a financial institution.[81]

*The Fair Credit Reporting Act*: This act establishes the guidelines that credit reporting agencies must follow and procedures for correcting your credit report.

*Electronic Funds Transfer Act*: This act provides for the protection of debit card transactions and other electronic transactions.[82]

*Fair Credit Billing Act*: This act provides for making corrections on credit card accounts.[83]

---

[77] Lazarony, Lucy. Identity theft serves up double threat to victims."
[78] "Identity Theft and Assumption Deterrence Act of 1998." URL: http://www.identitytheft.org/title18.htm (14 Nov. 2003).
[79] "PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON IDENTITY THEFT."
[80] "PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON IDENTITY THEFT."
[81] "PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON IDENTITY THEFT."
[82] "State and Federal Laws Related to Identity Theft" URL: http://www.identity-theft-protection.com/laws.html (14 Nov. 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Fair Debt Collection Practices Act: This act governs what a debt collector is allowed or not allowed to do.[84]

© SANS Institute 2004, Author retains full rights.

[83] "State and Federal Laws Related to Identity Theft"
[84] "State and Federal Laws Related to Identity Theft"

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

"ARM INTEGRITY TASK FORCE RECOMMENDATIONS ON BEST PRACTICES." 30 May 2003 URL: http://www.efta.org/new/FINAL_Report.pdf (16 Nov. 2003).

"AVOIDING CREDIT CARD FRAUD." family WATCH. Jan. 2003. Issue No. 16. URL: http://www.ccinsurances.com.au/publications/family_watch_issue_16.pdf (14 Nov. 2003).

"Beware of ATM Scams." St Cloud Federal Credit Union. Jan 2003. URL: http://www.stcloudfcu.com/newletter/2003_jan.pdf (14 Nov. 2003).

"Beware Scams At Your ATM." 21 Feb. 2003. URL: http://www.cbsnews.com/stories/2003/02/21/eveningnews/main541555.shtml (14 Nov. 2003).

"Card Fraud The Facts 2003." URL: http://www.cardwatch.org.uk/pdf_files/cardfraudfacts2003.pdf (14 Nov. 2003).

Card Skimming "Booming Cybercrime." URL: http://www.asianlaws.org/infosec/archives/07_03_card.htm (14 Nov. 2003).

“Financial Fraud: Important Lessons for Young Consumers.” Money Matter$, Fall 2003. URL: http://www.gettingfiscallyfit.org/highschool/fall03.pdf (16 Nov. 2003).

"How to be ATM "Streetwise"." URL: http://nsi.org/Tips/atmtips.html (16 Nov. 2003).

"Identity Theft and Assumption Deterrence Act of 1998." URL: http://www.identitytheft.org/title18.htm (14 Nov. 2003).

"New reasons to guard your ATM card." URL: http://moneycentral.msn.com/content/Banking/P57803.asp?Printer (14 Nov. 2003).

"PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON IDENTITY THEFT." 13 Sep. 2000. URL: http://www.ftc.gov/os/2000/09/idthefttest.htm (16 Nov. 2003).

"Public Alert." 15 Apr 2003. URL: http://www.wilmette.com/news/skimming.pdf (14 Nov. 2003).

"Shaping the Future of the Electronic Payments and Commerce Industry" URL: http://www.efta.org/welcome.htm (14 Nov. 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

"skimming is a scam." URL: HTTP://usa.visa.com/media/business/skim2.pdf (14 Nov. 2003).

"State and Federal Laws Related to Identity Theft" URL: http://www.identity-theft-protection.com/laws.html (14 Nov. 2003).

"What is identity theft?" URL: http://www.identitytheft.org/index.htm (14 Nov. 2003).

"What to do if you identity is stolen."25 Apr. 2003. URL: http://www.bankrate.com/brm/news/pf/20010301a.asp (14 Nov. 2003)

"What You Need To Know About Card Skimming." The Source. Summer 2003 URL: http://www.tcafcu.org/pdfs/SummerNews03.pdf (14 Nov. 2003).

"Wisconsin Bankers Association Warns Consumers, Asks for Help In Identifying ATM Card Skimming Scam." 7 May 2003. URL: http://www.wisbank.com/Media/Press%20Releases/PR_ATM_Card_Skimming_Scam.htm (14 Nov. 2003).

Aminu, Ayodele. "Association Raises Alarm Over ATM Fraud." 25 July 2003 URL: http://www.thisdayonline.com/archive/2003/02/05/20030205bus01.html (14 Nov. 2003).

Annese, John. "Customers reimbursed." 12 Aug. 2003 URL: http://www.zwire.com/site/news.cfm?newsid=10001183&BRD=985&PAG=461&dept_id=161556&rfi=6 (14 Nov. 2003)

Bruce, Laura. "Skimming the cash out of your account." 24 Mar 2003 URL: http://www.bankrate.com/brm/news/atm/20021004a.asp?prodtype=bank (14 Nov. 2003).

Costa, Christina. "MasterCard International Hosts First Global Risk Management Symposium." 13 May 2003. URL: http://www.mastercardintl.com/cgi-bin/newsroom.cgi?id=706 (16 Nov. 2003).

D'Angelo, Frank and Stephanie Cook." ATMs: Offering Convenience to Customers and Opportunities to Criminals." Aug./Sep. 2003 URL: http://www.wib.org/wb_articles/fraud_aug03/ATMs_aug03.htm (14 Nov. 2003).

Lazarony, Lucy. Identity theft serves up double threat to victims." 28 Apr. 2003. URL: http://www.bankrate.com/brm/news/pf/20010226a.asp (20 Nov. 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Milner, George with Sam Ott, Michele Petry and Mary Beth Guard. "Skimming, Scanning, and Scamming: ATM Crime On The Rise " 16 May 2003. URL: http://www.bankersonline.com/security/gm_atm_skimming.html (16 Nov. 2003).

Schmidt, Lucinda. " Warning signs." 15 Oct. 2003. URL: http://moneymanager.smh.com.au/articles/2003/10/15/1065917445606.html (14 Nov. 2003).

Tatum, Christine. "'Skimming' milks ATM customers cash." 1 May 2003. URL: http://www.chicagotribune.com/technology/local/profiles/chi-030501downloads,0,802804.column?coll=chi-shopping-hed (14 Nov. 2003).

© SANS Institute 2004, Author retains full rights.

Last Updated: May 22nd, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Malaysia @ MCMC 2013** | **Cyberjaya, MY** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **SANS Pen Test Berlin 2013** | **Berlin, DE** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **Industial Control Systems Security Training - Houston** | **Houston, TXUS** | **Jun 10, 2013 - Jun 15, 2013** | **Live Event** |
| **Security Impact of IPv6 Summit 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 16, 2013** | **Live Event** |
| **SANSFIRE 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 22, 2013** | **Live Event** |
| **SANS Canberra 2013** | **Canberra, AU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **SANS Thailand 2013** | **Bangkok, TH** | **Aug 19, 2013 - Aug 31, 2013** | **Live Event** |
| **SANS Virginia Beach 2013** | **Virginia Beach, VAUS** | **Aug 19, 2013 - Aug 30, 2013** | **Live Event** |
| **Mobile Device Security Summit 2013** | **OnlineCAUS** | **May 30, 2013 - Jun 06, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |