Hacking for Profit:

Credit Card Fraud

A Beginners Guide

by
SA E.J. Hilbert II
Federal Bureau of Investigation
Los Angeles Field Office
Santa Ana Resident Agency
714-542-8825
Written August 2002
Revised December 2004

Introduction

This paper is intended to detail how financially motivated hacking groups convert stolen data to monetary instruments. The primary premise for this paper is based on Eastern European hacking groups but in recent months, the "financially motivated" hacker sub group has expanded to include hackers from the Far and Middle East Hackers. What the individuals are doing with the illicit profits of their activities range from childish purchases to funding terrorist attacks as was detailed in the recent autobiography, "Aku Melawan Teroris" (Me, Fighting the Terrorists) by the Bali nightclub bomber. In the chapter "Hacking, Mengapa Tidak" (Hacking, Why not?), Iman Samura, a computer scientist provides a primer to Islamic Extremists of how to learn the trade of credit card fraud and hacking.

To quote BigBoss, from forum.Carderplanet.com, "Carding shouldn't be something you do for fun, it is something you do to survive."

Financially motivated hackers consider hacking and carding as their career. The employment opportunities are in their home countries, particularly those whose salaries are enough to pay for the life styles these individuals have become accustomed, are extremely limited. They come from a society where the average pay is $200 per month but Internet connectivity costs $40 per month. Thus they are willing to spend one fifth of their monthly salary to be online. A $1000 profit is more money then most Eastern European hackers have ever seen at one time.

Though they understand the process of credit cards, most International hackers do not understand the impact of committing credit card fraud. Most come from cash economies and the use of a credit card by regular citizens is extremely uncommon. They feel the attack is directed at a big corporation and not an individual. The idea of rising interest rates, chargeback fees or economic instability are not concepts they can understand nor are they their concern. Money is the object of their actions.

At the time of the first version of this paper in August 2003, many financially motivated hackers could be found chatting in the forums of the web sites carderplanet.com, shadowcrew.com and/or darkprofits.com. These sites are still referenced in this

paper because the information provided on the sites are still relevant.

Since that time, many of the referenced sites have been shutdown or taken over by script-kiddies and the real profiteers have moved deeper underground. Many have also become allied with organized crime groups or created their own hacking teams.

Also at the time of original publication, EFnet and DALnet on IRC initiated a crackdown on channels dedicated to cyber crime. Since that time, the criminals have found loop holes in the crackdown, such as renaming the groups, attaching messages of the day (MOTD)forbidding criminal activity or making the channels private. Many of the channels have also gone native; meaning they are dedicated to a particular language group and all posts to the channel utilize that language and the corresponding slang for carding.

The point being, the groups have not gone away. They still exist and communicate on the Internet by adapting to the rules. Law Enforcement must now adapt in kind.

By no means is this paper intended to be the end-all authority on this crime. Comments, questions and revision are always welcome.

Definitions, Concepts and Statistics

Since the readers of this paper will range from skilled investigators to neophytes, some basic terms and concepts need to be set forth:

Hacker – Individual who gains unauthorized access to computer networks and systems

Carder – Individual who uses stolen data, usually Credit cards, to fraudulently purchase items or convert the credit into cash.

Credit card – a monetary instrument, often referred to as plastic, used in place of cash to make purchases. Credit cards are assigned to entities and have specific monetary limits and an interest rate associated with payoff. Since credit cards do not have to be paid off each month, the available limit will fluctuate. Visa or MasterCard does not issue Visa and MasterCard credit cards. They are issued by an issuing bank in conjunction with a use agreement between the bank and Visa or MasterCard.

This agreement is for the use of the Visanet or the MasterCard equivalent for verification and authorization of the card.

Charge card – same as credit card however, a charge card must be paid off each month or risk an extremely high interest rate or the card being shutdown.

Debit Card – Card associated with a bank account and limited by the amount of money in said account, which resembles the credit card by the method of purchase. However, these cards may only be used with the owners Personalized Identification Number.

Hacker knowledge

Below is the "Beginning Carders Dictionary'" as posted online by the Russian hacker, KLYKVA on forum.carderplanet.com. It is presented in its original form to illustrate the level of knowledge from which these individuals are working.

Bank-emitent (Issuing bank) – bank which has issued the card

Billing address – the card owner address

Drop – innerman. His task is to receive the money or goods and, accordingly, give the part of the earnings to you.

Drop/Pick-Up guy/Runner – person or location that is setup to accept packages or to receive the money. He should be paid nicely for this position.

Billing – office, which has agreement with a bank and assumes payments for the cards.

COB – Change of Billing address

Card bill – a Bank emitent card bill.

Bank-aquirer – bank, in which the store opens the account.

Merchant account – bank account for accepting credit cards.

Merchant Bank – bank, through which occur the payments between the buyer and the seller (frequently it is used as synonym "bank-equirer").

Cardholder – owner of the card.

Validity – suitability of card.

White plastic – a piece of pure plastic, where the information is plotted/printed.

CR-80 – rectangular piece of pure white plastic (without the drawing image) the size of a credit card with the magnetic strip.

Transaction – charge to the credit card

POS terminal (Point Of Sale terminal) – reading card device, which stands at commercial point.

PIN-code – (Personal Identification Number) the sequence, which consists of 4-12 numbers, known only to the owner of card. A simple word password for an ATM and so on.

AVS – the card owner address checking. It is used for the confirmation of the card belonging exactly to its holder.

“Globe” – card holographic gluing with the image of two hemispheres (MasterCard).

Pigeon (hen) – card holographic gluing with the image of the flying pigeon (VISA).

Reader – information reading device for the readout from the magnetic strip of card.

Encoder – read/write device for the magnetic track of the card.

Embosser – card symbol extrusion device.

Card printer – card information printing device.

Exp.date – card validity period.

Area code – the first of 3 or 6 digits of the card owner’s phone number.

CVV2, cvv, cvn – 3 or 4 additional numbers, which stand at the end of the number of card.

ePlus – program for checking the cards.

BIN – first 6 numbers of the card number which make it possible to learn what bank issued the card and what type of card (ATM-card, credit, gold, etc.). Synonym of word “Prefix”.

Chargeback – the cardholder’s bank voids the removal of money from its card.

Dump – information, which is written to the magnetic strip of the card, it consists of 1,2 or 3 tracks.

MMN – Mothers Maiden Name (generally the primary account holders mother)

Track (road) – a part of the dump with specific information. Every 1st track is the information about the owner of the card. 2nd track – information about the owner of card and about the bank who issued the card, etc. 3rd track – it is possible to say – spare, it is used by stores for the addition of the points and other.

Slip – synonym to the word “cheque” (conformably to card settlings).

Card balance – amount of credit remaining for spending in the card account.

Automated Clearing House (ACH) – the automated clearinghouse. The voluntary association of depositors, which achieves clearing of checks and electronic units by the direct exchange of means between the members of association.

Continuous Acquisition and Life-cycle Support (CALS) – the integrated system of the production guaranteeing, purchase and exploitation. This system makes possible to computerize all data about the design, development, production, servicing and the propagation of the production.

Debit Card – Card, which resembles the credit card by the method of using, but making possible to realize direct buyer account debiting at the moment of the purchase of goods or service.

Delivery Versus Payment (DVP) – the system of calculations in the operations with the valuable papers, which ensures the mechanism, that guarantees the delivery will occur only in the case of payment and at the moment of payment.

Direct debit – payment levy method, mainly, with the repetitive nature (lease pay, insurance reward, etc.) with which the debitor authorizes his financial establishment to debit his current account when obtaining calculations on payment from the indicated creditor.

Electronic Fund Transfer (EFT) – the remittance of means, initiated from the terminal, telephone or magnetic carrier (tape or diskette), by transfer of instructions or authorities to financial establishment, that concern the debiting or crediting of the account (see Electronic Fund Transfer/Point of Sale – EFT/POS).

Electronic Fund Transfer/Point of Sale – EFT/POS – debiting from the electronic terminal, for the transfer purpose from the account of a buyer into the payment on the obligations, which arose in the course of transaction at the point of sale.

Integrated Circuit (IC) Card – It is known also as chip card. Card equipped with one or several computer micro-chips or integrated microcircuits for identification and storing of data or their special treatment, utilized for the establishment of the authenticity of personal identification number (PIN), for delivery of permission for the purchase, account balance checking and storing the personal records. In certain cases, the card memory renewal during each use (renewed account balance).

Internet – the open world communication infrastructure, which consists of the interrelated computer networks and provides access to the remote information and information exchange between the computers.

International Standardization Organization (ISO) – International organization, which carries out standardization, with the staff office in Geneva, Switzerland.

Magnetic Ink Character Recognition (MICR) – System, which ensures the machine reading of the information, substituted by magnetic inks in the lower part of the check, including the number of check, the code of department, sum and the number of account.

RSA – the coding and authentication technology, developed in 1977 in MIT by Rivest, Shamir and Adel’man, which subsequently opened their own company RSA Data Security, Inc., purchased recently by the company Security Dynamics Technologies, Inc.

Real-Time Gross Settlement (RTGS) - the payment method, with which the transfer of means is achieved for each transaction in obtaining instructions about the payment. Decrease the risk with the payment.

Smart Card - card equipped with integrated circuit and microprocessor, capable of carrying out the calculations.

System risk - the risk, with which the incapacity of one of the payment system participants either financial market participants as a whole to fulfill their obligations, causes the incapacity of other participants or financial establishments to fulfill its obligations (including obligations regarding the realization of calculations in means transfer systems) properly. This failure can cause significant liquidity or crediting problems and, as result, it can cause loss to the stability of financial markets (with the subsequent action on the level of economic activity).

Truncation - procedure, which makes it possible to limit the physical displacements of a paper document (in the ideal version) by the bank of the first presentation, by the replacement by electronic transfer of entire or part of the information, which is contained on this document (check).

Card Balance - Current used Credit

Avail Credit - Actual credit avail for Spending

Cash Advance Avail - Actual amount avail as Cash for ATM usage.

Integrated Circuit (IC) Card - It is known also as chip card. Card equipped with one or several computer micro-chips or integrated microcircuits for identification and storing of data or their special treatment, utilized for the establishment of the authenticity of personal identification number (PIN), for delivery of permission for the purchase, account balance checking and storing the personal records. In certain cases, the card memory renewal during each use (renewed account balance).

LE - Law Enforcement, Coppers, Piggies, The Fuzzzzzzzzzzz

Lappie- Laptop

Communication Methods

As in all endeavors, hackers and carders need a means or several means of communication. Given the international make-up

of most hacking groups and the fact of Cyber crime being truly borderless, the communication methods chosen by these groups must be internationally accessible, cost effective and have a high level of anonymity. Listed below are several of the primary communications methods used by hackers and carders:

IRC – Internet Relay Chat, a series of interconnected computer servers on various network which enable users to chat in channels and one to one. The channels are also referred to as rooms and are controlled by the user who first established the room.

ICQ – America Online (AOL) owned peer-to-peer chat application. Chat rooms can be established within the ICQ network but entrance is by invitation only.

AIM– AOL Instant Messenger

Forums – Website sponsored bulletin boards where public and private messages can be posted about various topics. Examples: forum.carderplanet.com, eraser.hostmos.ru, www.darkprofits.com and www.carderclan.net

Email – Electronic mail

A Credit Card (VISA) Transaction

There are two parts to every transaction. First, a customer presents a Visa product, usually a card, to a merchant, who needs immediate authorization of the transaction. Second, at the end of the day, the merchant needs to receive the funds for the transaction via its financial institution and ultimately from the customer's issuer. The specifics will vary depending on transaction type, complexity, technology, and processing services but the typical flow is illustrated here.

How a Purchase is Made

Authorization at the Point of Sale

Maria presents a Visa card (credit or debit) at ABC Stores. ABC uses an electronic terminal or the telephone to request an authorization from its financial institution (DEF Merchant Services).

DEF checks to see if the account is valid and has sufficient funds. It sends an authorization request message, including

owner's account, merchant account and transaction details, through VisaNet to GHI Bank, Maria's Visa issuer.

GHI reviews the request and makes a decision to approve or decline the request. GHI's response message is sent back through VisaNet to ABC within seconds.

In some cases, when an issuer is unavailable for authorization, VisaNet will authorize the transaction as part of a Stand-In Processing Service. This is done to further enhance payment system efficiency. The entire authorization process, when done electronically, takes about two seconds.

How the Merchant Gets Paid

Clearing and Settlement

At the end of the day, ABC Stores delivers all its sales draft information (including Maria's purchase) to DEF Merchant Services. Each draft will contain the credit card number and the merchant account number. DEF credits the merchant account of ABC Stores for the net amount of all its sales. This is how ABC Stores obtains its funds from Maria's purchase.

Next, DEF's processing center creates an electronic version of all drafts for all the merchants it supports, including ABC Stores. The electronic drafts, which may include transactions from numerous Visa account holders in various countries, are sent through VisaNet to one of Visa's data centers.

Visa routes these drafts to the financial institutions of the Visa account holders, for instance, Maria's transaction is sent to her issuing bank, GHI Bank. Visa consolidates all transactions for each issuer into an electronic file that includes currency conversions, fees, net settlement amounts, and required reporting information.

GHI's processing center receives the file and prepares the transactions for posting to its cardholders' accounts including Maria's.

GHI Bank transfers all the funds owed that day by its cardholders, including Maria, to a settlement bank, which is responsible for delivering the funds to the merchant acquirers such as DEF Merchant Services. This is how DEF gets paid for the amount it paid ABC Stores in step #2.

At the end of the billing period, GHI Bank produces a statement to Maria. This is how GHI settles with Maria.

Statistics

Visa annual worldwide sales volume exceeds US$2.4 trillion. There are 1.2 billion Visa, Visa Electron, Visa Cash, Interlink and PLUS cards worldwide. But only 49,413 legally issued cards in Central Europe, the Middle East and Africa.

Visa is accepted in more than 150 countries.

As of March 31, 2003, MasterCard's gross dollar volume for credit and debit programs was US$285.7 billion, an increase of 7.31% over the same period in 2002.

MasterCard has 32 million acceptance locations; no payment card is more widely accepted globally.

Cardholders can obtain cash with the card at bank branches and at all ATMs in the global MasterCard/Maestro/Cirrus ATM Network, among the largest ATM networks in the world with more than 892,000 ATM locations worldwide on all seven continents.

Most Eastern European law enforcement officers do not own, use or understand a credit card. This is important when requesting information from certain parts of the world. All requests must be highly detailed and precise.

What to Steal

Everything is worth stealing to these individuals. These hackers are financially motivated and highly educated. They are not the typical hackers found in the U.S. Hacking and Carding is a business for them. They hack to steal databases, which in turn are provided to carders. Carders, utilizing various schemes convert the stolen credit cards to cash or equipment then, provide the cards freely online in carding related IRC chat rooms. The intention of the free cards is to spread the information as widely as possible thus making it difficult for law-enforcement to track who originally committed the hack.

The hack occurs in three parts, reconnaissance, theft and dump. During the reconnaissance portion, the hackers steal everything. This information is used to identify the important parts of the network, the location of the databases and user names and passwords. The reconnaissance usually occurs two to three

months before the theft. During the theft portion, the hacks begin to glean specific information, i.e., credit card numbers from the system as needed. The theft phase can last for years and the hackers usually leave a very small footprint of their activities. The dump stage occurs when the hackers steal everything in a very “noisy” manner. This stage is used to burn all those “script-kiddies” and “lamerz” who are taking advantage of the original hackers backdoors. The dump phase usually results in press coverage and the “red-flagging” of all the credit cards in the system at that point in time. The victim company makes security changes and over time lets their guard down. The hackers then attempt to use the old backdoors they created. If they are still in place, the theft stage begins again.

The hacks normally take advantage of known vulnerabilities, which have not been patched by the various victims. Most hacks occur against Microsoft Windows platforms and utilize the Msdac exploit, the MSSQL exploit or the IIS exploit. A wealth of information is available about these exploits on the Internet.

The truly skilled hackers have developed their own tools and place backdoors on systems such as, installing Telnet and secure shell daemons on high port numbers or creating their own user id’s and passwords after installing a sniffer to steal the root level passwords. These are the first things System Administrators should look for, as well as changing all root level passwords via face-to-face meetings with all root level users. Sending the change of passwords via email will be intercepted if a sniffer has been installed on the system.

Sometimes, the hack is automated through the use of a “bot” which makes it impossible for the System Administrators of the victimized networks to stop because they are physically not fast enough to fight the bot. The only way to stop the bot is to take the network offline.

Investigations thus far indicate the following items are being stolen for use in various schemes detailed later in this paper:

- Credit card databases
- Personal information (name address telephone numbers)
- Bank accounts
- Bank routing numbers
- Social Security numbers
- Email addresses and passwords

- Computer logon names and passwords
- ACH transfer records
- Merchant accounts
- Order histories
- Client lists
- Partner lists
- Company telephone directories
- Website Source code
- Shipment tracking numbers
- Ebay accounts
- Escrow accounts
- Proprietary Software

Getting Credit Cards

Of all the data sought by hackers, credit card databases are the highest priority. This is because they are the easiest to use.

There are nine basic methods to obtain credit card numbers:

Phishing – This is the practice of sending fraudulent e-mails that appear legitimate. The email often appear to be from a bank or financial institution and request the recipient update their account information by utilizing the link included in the email. The link takes the recipient to a bogus web page where all the requested information is captured and later transmitted to a site controlled by the criminal for their use in cyber crime. Amongst the information often requested is the recipients social security number, credit card number, PIN and cvv2.

Buy – There are literally thousands of "Vendors" on web sites such as Forum.carderplanet.com, darkprofits.net and Shadowcrew.com willing to sell dumps of credit cards at varying rates. If a carder knows how to use cards, expending $200 up front for cards is easily recouped.

Trade – Through the different communication methods discussed above, hackers and carders trade credit cards online. Many cards are offered free of charge. The individual who stole the cards often has used these cards for fraudulent purchases. They are then offered to the community as a whole with the intention of having multiple people use the cards. Law enforcement will therefore have a harder time identifying the original hacker from the various carders.

Generate – There are numerous software packages freely available on the Internet, which generate credit card numbers. Many of the programs use the DESIII algorithm just like the legitimate credit card companies.

The problem for the carder with generated cards, is that approximately 1% of the cards are valid. This means the carder will need to have access to obtain validity and authorization before trying to commit fraud. A common method would be a merchant account.

Visa and MasterCard do not issue or generate cards, however they allow banks to issue cards with the respective logos/brands. American Express differs from Visa and MasterCard in this respect. American Express controls all cards and card numbers using their logo. American Express actually generates card numbers in advance, which are stored in an active state awaiting issuance to a customer. If a carder generates one of the stored American Express cards, any merchant receiving the card for payment will receive authorization for the purchase.

Extrapolate – Once a Carder obtains a valid card through any of the different means listed herein, he can extrapolate additional cards based on the valid card number and the expiration date. Various extrapolation programs are freely available on the Internet. These programs utilize the valid card as a base for creating additional cards, particularly the first six digits. Extrapolation increases the likelihood of obtaining valid credit cards to approximately 35-40%. Once again a method to determine the validity via authorization is required.

Fake Shops – It seems every business must now have a presence on the Internet in order to do business. Couple this fact with the general publics' belief that web sites are not easy to set up. It is not difficult to understand why many feel if the company has a nice web site, the company must have money and be a reputable company. Many hackers and carders will use these beliefs to their advantage by setting up fake online shops offering products for sale at cut-rate prices. Good hackers and carders will spend the extra time to post fake recommendations on rating sites to help move their fake shop into the top ten slot on search engines. When customers place an order at the shop, they will be informed via email, their product will be shipped in 4-6 weeks. While the customer is waiting for their product, the shop owners continue to collect credit card numbers. At this point there are three possible scenarios:

The first is that the product is simply not shipped and the credit card is never charged. The second is the product is not shipped but the credit card is charged. In the third scenario, the product is shipped and the customer is happy. The details of this scheme will be covered in depth later in the paper but, in all three scenarios it should be noted, the hackers and carders received legitimate credit card numbers with full information.

Intrusions – The method of obtaining credit cards that has received the most press is Intrusion. The hacker simply gains unauthorized access to a system and steals the database. The systems targeted by hackers include the following:

- Online shops running shopping card programs
- E-Commerce payment solution sites which handle online orders for online shops
- Credit Card processing companies such as Authorize.net, creditcards.com and CCBill.com
- Online monetary exchange sites where a person can purchase monetary units using credit cards
- Online Casinos
- Pornographic websites (victim often do not notify Law Enforcement of intrusions)
- Banks and Financial institutions

Each of these targets will have credit card information stored in some variation. Some will include full information including CVV2 numbers while others will simply store the credit card number and expiration date.

Identity Theft – This method is labor and time intensive but, once the credit card is obtained, the card is valid and often has a high credit limit. Using stolen identities, the carder simply applies for a credit card. How the identities are obtained range from simply web searches to buying access to ChoicePoint or Lexus/Nexus gaining data from their databases.

This scheme will also be covered more in depth later in this paper.

Social Engineering (SE) – By far the most low-tech method of obtaining information, the hackers and carders will simply try to get the individuals to provide the information. This is done through telephone calls, faxes or email. A very common SE method

is the email sent to particular customers stating there is some issue with their account. The customer is asked to log on using the link contained in the email. Once the customer logs on, all the information they input into the web site is collected for use by the hacker. When the individual selects the submit button on the web page, a message stating some computer glitch appears and the customer is asked to select the continue button which will re-direct the customer to the legitimate site and the customer re-enters their information. This time, the proper site accepts whichever change the individual makes, and the customer has unknowingly provided the hacker/carder with full account information.

This method has been reportedly used for gathering email, Paypal, bank and credit card account information.

The Schemes

Each hacking and carding group try to develop their own original scheme to make money from the stolen data however, there are several primary schemes for converting stolen data into cash or product upon which all the others are based. Below, the primary schemes and a few widely used variations are detailed. It is important to note, the variations are only limited by the imagination and knowledge of the subjects.

Sell - The easiest and quickest method to make money from stolen cards is to simply sell them online. The sale of card data is called a "dump" in which the hacker/carder offers the data for trade or sale, often track 1 and 2. The going rate online is approximately $.35-$.50 for credit card numbers and expiration dates. Cards with full subscriber information and CVV2 numbers range in price from $2.00 to $4.50. Also cards are sold based on their verified credit line i.e., $100 for a card with an available credit line of $10,000.

Auction Fraud - Also an incredibly easy scheme, auction fraud has been somewhat limited by the establishment of online escrow companies. But note, fake online auction companies can easily be created as well. In this scheme, the subject simply posts a fake auction item and sells it to the highest bidder. The buyer sends the seller money or a credit card number but never receives the product.

A couple variations of this scheme are as follows:

A. The hacker/carder uses the stolen credit card to make purchases of auction items. This can be done on a person-to-person sale or through the use of an escrow account. If an escrow account is involved, the hacker/carder will either open an escrow account based on the stolen information or will steal an escrow account and use whatever funds are in the account to make purchases. The purchases will be shipped to a drop and picked up later by either the subject or his associate to be re-packaged and shipped elsewhere, usually overseas. The use of a drop and an associate is called a trans-shipper. How trans-shippers are obtained is discussed later.

B. The second variation is more sophisticated and forces the escrow account to serve as a money laundering conduits. The hacker/carder will open several escrow accounts, one based on a bank account controlled by the hacker/carder and the others based on stolen credit card or bank account information. Often times neither account is in the subject's true name.

The real account is used to post numerous online auctions. The auctions take place for a limited period of time and the hacker wins his own auctions using one of the fraudulent accounts. This fraudulent account is then used to pay the escrow company. The seller informs the escrow account the product has been sent, the buyer states he received the product and instructs the escrow company to release the funds. The funds are transferred to the real escrow account from which they are immediately withdrawn and transferred to a bank account or withdrawn via an ATM. At no time during the transaction did any product change hands. All the money was transferred via the escrow company thus, in 30-days when the card holders whose cards were used for the fraudulent accounts file chargebacks, the chargeback is sent to the escrow company.

Fraudulent Purchases - This scheme is also simple in that the hacker/carder simply makes a purchase online using the stolen credit card. The difficulty for this scheme is that merchants often will not ship overseas therefore, the subjects need an address within the U.S. to which to ship the product.

On Fraudulent Purchases the hacker/carders need a drop, a person or location to send the packages without identifying themselves. Drops can be obtained in various ways.

A. The most common is to post on a hacker/carder forum the need of a partner and establish a working relationship with whoever answers the postings.

B. Drops can also be obtained by posting a job offer on Hotjobs.com or Monster.com for an individual to work at home. Individuals will be paid via Western Union to accept and repackage items and send them overseas. A skilled Social Engineer can convince people of the legality of accepting packages in this method and the newly hired employee is unaware they are facilitating a crime.

When it comes to paying these employees, the hackers/carders vary as well. Many will simply not pay their employees and leave them "holding the bag" when complaints are filed. Others choose to pay their employees through Western Union. Still others act as if they are paying the employee by sending them a counterfeit check. The checks will be drawn for substantially higher amounts then are owed the new employee. When the employee comments regarding the value of the check, the employer states it was an oversight and asks the employee to simply wire the employer the remaining funds after the subtraction of the monies owed the employee plus a bonus for being honest. The employee sends the wire transfer overseas and two to three days later finds out the check is counterfeit. The employee is not only out their salary but additionally the amount wired overseas.

B. The third variation is called COB (change of billing). Most credit card companies allow their customers online access to their account. With this online access, the customer can change billing addresses; telephone numbers, passwords and so on. The intriguing aspect is that most people do not activate their online access. When a hacker/carder steals a credit card with full information, they can then go online and change the billing address to match that of one of the drops they control. The COB is extremely useful when the company the items are being purchased from, will only ship to the billing address.

C. If the drop is worried about having the packages shipped to their address, P.O. boxes are used and an ingenious method is to send the packages to vacant homes. An individual can contact a local real estate agent to determine which homes are for sale and when the occupants plan on moving out. During the brief time the house is vacant, the drop can simply pick up the packages from the mailbox of the vacant house.

D. A final variation involves some sophistication, but it limits the need for an associate. When an item is fraudulently purchased, the hacker/carder has the package shipped to the credit card holder's real address. A slow shipment method is requested as well as a fax or email of the scanned shipping bar code. When the hacker/carder receives a copy of the shipping bar code, they can utilize a bar code scanner to read the code. They then contact the shipping company, provide the information contained in the bar code and a change of the shipping location. The new cost for the shipment is billed to the defrauded company or can be charged to another stolen credit card.

Below is a post by a carder named JediMasterC detailing how to card in the real world based on dumps of credit cards obtained online or through skimming:

Mon Jul 21, 2003 11:41 am Post subject: TUTORIAL - Carding with Dumps July 21 2003

This is dedicated to cumbajonny and other people who watch their backs closely. If you're that careful you will probably never be caught. The date in the topic will be changed whenever there is an update

Disclaimer
This document was written for informational purposes only. It was written so that credit card companies, banks, merchants, retail stores, and the consumer will have a better understanding on how these activities work and how to protect themselves. I have never participated in any of the described activities and am not suggesting that anyone else should either. All described acts, memories, quotes, and ideas are fictional.

Intro
So, you've heard all kinds of things about carding with dumps and you're interested, but you don't know where to start. Look no further than this tutorial. Written by JediMasterC for carderplanet.net, this tutorial will tell you everything you need to know from beginning to end. Feel free to distribute this document, so long I am given credit. I can be contacted on CarderPlanet.

Newbie Warning
If you are new to credit cards do not even think of doing anything here until you have more experience. It may seem easy (and it is), but you must have certain mindset. The key to success, at anything in life, is knowledge and the ability to apply your knowledge. Anything done in person takes a little more than that. It takes presentation. It takes charisma. It takes charm. If you're a pimply 16-year-old wearing cut offs and a sleeveless shirt, do you honestly think that someone will believe you can afford a $3000 computer system? It's possible, if you know how to act and what to say. As a newbie you know nothing about the life, how "carding" works, how cards work, etc. Learn everything you possibly can before you step out into the real world, and then start small.

How to start
You must have some money saved up in order to start in this business (or be really good at online carding). I assume you have some sort of transportation, a computer, and some brains. Let's take a look at a list of other things you will need (all costs are approximate):

Card encoder - Get an MSR206. It is the standard when it comes to encoders. I have heard that the AMC-722 works, but it will not last as long and will break. There are a few online places that sell the MSR206. I bought mine new with my own card and money. Cost: $725 new (around $500 used) Hard to card.

Laptop - You may not need this to get started, but you'll find out quickly that it will save a lot of time. If you don't have a laptop you will need to go home every time a card dies. I suggest the smallest, lightest laptop possible. Cost: $500-$2000, cardable.

Serial to USB Adaptor - Most encoders are serial based (including the MSR206), and most small laptops don't have serial ports. Get a USB adaptor to make it easier on yourself. Cost: $10-$25, cardable.

Power Inverter - You'll want to power your encoder in your car, and for that you'll need a power inverter. Sure, the MSR206 is 12v and you could make an adaptor, but where are you going to find the strange connector it uses? You'll probably use the power adaptor for other things anyway. For an encoder or laptop a small one will do, say 75-100 watts. Cost: $25-$55, cardable.

Credit Card to encode onto - You'll need something to put those dumps on, and it's not a blank white card. You'll need to get a card from somewhere. I have found a great way to handle this, see below. Cost: $0-$25

Dumps - Duh! You'll need these! There are a few vendors on CarderPlanet, see the Vendors forum for a list. Most have minimum orders, and there are different types you can choose. Don't worry about a minimum order; you'll make your money back quickly. We'll talk about types (Classic, Gold, etc) later. Cost: $200-$500 to start, much more in the future

Fake ID - While it is not necessary right now, you'll need one when making large purchases. I have tried going without one and was never rejected because I didn't have it, but it will make things much more smooth. If you have never made one before, don't start now. They are easy once you get enough practice, but you don't want to be using a really bad one for this. Buy one from a vendor on CarderPlanet. More later. Cost: $5 plus equipment and time to make yourself, $75-$150 to buy.

These are the things I suggest you have when starting. While you can go without a laptop, power inverter, and fake ID if you are very short on funds, I suggest you save up and start correctly. Once you start and get the hang of it, here are a few things I suggest you get while out on a mission:

Anon cell phone - Use to check dumps with phone merchant.
Extra wallet - Keep the fake stuff and your real stuff separate.
Case for laptop/encoder - I suggest using a briefcase to carry them. All you have to do is pop it open, hook a few cables up, and go. You won't have to dig in a bag to pull everything out.

Where can I get a card to use?

So, you want to know where you can get a credit card to use for encoding. Don't use a stolen card!! I cannot say that enough. At some time the card will get typed in or phoned in, and it will come back as stolen. Do not use your own card, or they will have your name and info. If you were thinking of using your own card stop reading this right now, close your web browser, and get back to a real job. You are not cut out for this and you WILL get caught. Now, back to where you CAN get a card. There are a few options. I like prepaid cards. Depending on where you live, you can get prepaid credit cards out of a machine, at a mall, or at a convenience store. Simon Malls (www.simon.com) have gift cards that are prepaid Visa cards. There are many banks that have them now too. If you can't find a place to buy one in person, you can get a drop and order one. Try www.mymccard.com, www.storedvalue.aaa.com, or some other similar product. If you have to order one that will have a name printed on it, make sure it's the same as your ID. Do not order one to your house; do not use your own card to order it, etc. If you were thinking of doing that quit now before you get caught. I also like to have two cards with me, in case the one I'm using gets declined. That way I can just say "Let me try my other card" and hand them that one, instead of saying, "Oh, I'll have to come back later".

Kinds of dumps
So, what kind of dump should you use? It all depends on what you will be buying. If you plan on buying a lot of lower priced things (less than $500), go with Classic. They are the cheapest, but have the lowest limits. You can eat through a list of classic cards very quickly. If you plan on making larger purchases go with gold, platinum, or signature. I stick to Visa/Mastercard. Many stores require the CVN of an Amex card (number printed on front), and it will look strange when the computer says you used an Amex and you're holding a Visa/Mastercard.

Track 2 or 1 and 2?
Again, this depends on where you will be using it. Most places use both tracks. See list below for places that use only track 2. Remember, stores are always updating their systems so this could change at any time. I suggest always using both, although sometimes you can get very good deals on dumps with only track 2.

I'm ready, now what?
So you have everything you need, or do you? How about software for your encoder? I use TheJerm's MSR206 program. You can download it at http://www.thejerm.0catch.com/. It's easy and it works great.

Now, before you encode your card you have to change the name. Put the name on it from your fake ID. If you look at the dump you'll see something like this:

B4111111111111111111^SMITH/JOHN^03071010000000000000000000
4111111111111111111=03071010000000000000000000

It's not hard to figure out where the name goes. The numbers right after the name in track one and right after the = in track two is the exp date in YYMM format. This card would expire July 2003. The rest is the bank data, which we won't get into here.

So, change the name and encode. Now you're physically ready. Are you mentally ready?

Prepare your mind
You ARE the person on your ID. This is YOUR credit card. You are buying something you saved for. It is YOUR money you are spending.

These are things you should be thinking. The more you believe this the easier it will be. If anyone ever questions you react like they are crazy.

What do you mean? This is my card! Do you want to see my ID? I've been saving a long time for this! Fine, I'll spend my money at another store!

Always think about any possible situation. You will have cards declined frequently. I like to make the nice person at the register think it may be declined before I even use it. I'll say something like "Ohhh, I didn't think it was that much. I hope I have enough left to buy it!" They will expect it to be declined and think nothing of it if it is. If it goes through they will smile and laugh. Sometimes I won't say anything beforehand. If it gets declined I'll make up some excuse like "I must be over my daily limit" or "My payment must not have gone through." Always think about what to say before you have to say it.

Another thing to remember: DON'T PANIC! DON'T PANIC! DON'T PANIC! Even when things seem to be going wrong keep your cool. Cashiers always think there is something wrong with the system, or that there is a problem with the bank, etc. As long as the card you have encoded the dump onto isn't stolen you won't have any problems. Even when the computer tells them to pick the card up cashiers never do it. Just say you'll take the card and call the bank and work it out. They will hand it right back to you.

Posted: Fri Jul 25, 2003 12:54 am Post subject: Continued...

Shop shop shop!
Now go shopping! Start small and work your way up. I almost always go to a grocery store first; just to make sure the dump is working 100%. This is really unnecessary, but you have to eat anyway. Almost all grocery stores have self-swipe card readers that will help you get comfortable. Make sure you sign the name on the card and not your real name! I would suggest that you don't go to gas stations. While it seems like an easy way to check the card and everyone always needs gas, there are always tons of cameras there. The chances of them linking the card to you and to your car are very low, but there is a chance. Spend the $20 and just make it back at the next store you go to! ALWAYS MAKE SURE TO PARK FAR AWAY FROM ANY CAMERAS! You don't want your plates caught on the security camera! Some people put fake plates on their car. Better to be safe than sorry!

Where should I shop?
This all depends on where you live what you want to buy. Always scout out a new store before shopping. Why? Because there is one thing that can catch you: the last 4 digits of the card. Some stores will swipe your card and then type in the last 4 digits embossed on the front of the real card. If they don't match then there is a problem. It's easy enough to spot. Watch the cashier swipe a card. If they look at it and then type stuff in, they are probably doing what I just described. So, which stores check and which don't? Here's a list of stores I have found that do and do not check. This is a brief list off of the top of my head, I will try to improve it frequently. Always scout them out before you go there, since stores change their policies frequently.

Stores that DO NOT type them in:

Abercrombie & Fitch
Aeropostale
Almost every clothing store*
American Eagle
Barnes and Noble
Bose Factory Store/Showroom
Burlington Coat Factory
Eddie Bauer
Every gas station (pay at pump)*
Every grocery store I have ever been to (many self swipe)
Foot Locker
FYE
Gap
Home Depot (self swipe)
JCPenny
Kauffman's
Kmart (self swipe)
Lowe's (self swipe)
Office Depot
Old Navy
Sears
Spencer Gifts
Staples*
Target (self swipe, sometimes check sig)
Toy Works
Toys R Us
Walden Books
Walmart (self swipe but most check sig)

Restaurants:
Applebee's
Olive Garden
Pizza Hut
Many other large chains

*There is only one clothing store I have gone to that typed them in. It was an outlet store, but I do not remember the name. It has been reported that in some areas Staples types them in. Some gas stations ask for your billing zip code.

Stores that DO type them in (AVOID!):

Circuit City
Best Buy
CompUSA
OfficeMax

Remember, always scout out the store before shopping.

DO NOT SH** WHERE YOU LIVE! Don't shop at home, especially if you live in a small town. If you're in a city it may be alright, just don't go to the places frequently shop with your own card or money. Some people say you should never go to the same place twice. I say this is BS. I have been to some places 50 times without any problems. The store don't really care, they get to keep the money. Most of the time the stores don't even find out about it. Just make sure you are a typical customer that doesn't stick out. Wear plain, normal clothing, Smile, be polite, and you should have no problems. You want to be able to go to the

same place a few times a week without being recognized. Only then are you truly a successful confidence man.

What now?
So now you know how to buy things. The best way to make money is to sell items on Ebay that are in high demand. You can do your own research into this.

Another Option
Another option that was not covered here is buying or making fake cards. There are a few vendors on CarderPlanet that sell them, but making them is a whole other topic. This may be a safer route for you to explore. You would not need to buy any special equipment, but if a card goes bad before you use it you're usually stuck (some vendors replace them).

Conclusion
This should have given you an overview of how to carry out one of the most profitable and least dangerous methods of carding. You can easily live for free, have a steady income, and have fun.

I am always trying to improve everything about myself, including this document. Check back to http://forum.carderplanet.net frequently for updates.

This post was provided as a tutorial and had numerous post clarifying details of the scam as replies to the original post. This scheme should be considered when conducting a search of a known carder. It is likely the credit card in his/her possession may be coded with the card number of a dump rather than the number embossed on the front of the card.

Merchant Account – One of the more popular schemes is Merchant Account fraud. In this scheme, the hacker steals the credit card database of one company and the merchant account of a second. The carder charges an amount on each card to the merchant account. Once the charges have cleared, approximately one hour later, the carder issues a refund from the merchant account for the total amount charged on the cards to the hacker controlled debit card account overseas. A “drop” is then used to retrieve the stolen money from the ATM using the hackers’ debit card and the money is forwarded via Western Union, Money Gram or Webmoney to the hacker.

Often times the money is bounced through several bank accounts before reaching the hacker/carder or the hacker/carder will forego the use of a drop and pick up the money themselves. The victim is not aware of the charges and the refund until their merchant account is reconciled, usually at the end of the month. When the card members notice the unauthorized charges on their cards, they request the charges be canceled. This results in a

charge back to the merchant for the cost of the charge as well as a fine for bad charges.

Western Union/Money Gram/Egold – This scheme is similar to fraudulent purchases however, the purchase is credits, which can be translated into cash or traded for goods. Basically the hacker/carder uses the stolen credit card as collateral for online monetary units such as money orders, Egold dollars or Webmoney dollars. The use of these monetary mediums is expensive in terms of fees and percentages but, since the money is stolen in the first place, hackers/carders do not complain about the charges.

A hacker/carder can use these online dollars to purchase money orders at Western Union and have the money orders forwarded to companies to pay for goods and services. A notable purchase through money orders is the monthly payment for maintenance of websites associated with hacking or carding.

Bank Attacks – Bank account information can be used for opening escrow accounts, online brokerage accounts (i.e., E*trade, Datek or Ameritrade) or initiating wire transfers. Currently, most banks with online presence do not allow wire transfers online for the regular customer. However, brokerage accounts and corporate accounts issue credit cards and do allow online wire transfer requests. These accounts often have a significant credit limit or bank balance. These are the targets of the truly financially motivated hackers and their organized crime backers.

In order to cause a wire transfer to travel overseas, the hackers will have to compromise the SWIFT transfer system. It has been reported online, several hackers have found a way to compromise the system but no reported cases have been found.

For wire transfers in the United States, the Automated Clearinghouse (ACH) network is used. A hacker who has researched the ACH system could cause an ACH re-route to occur thus, having money deposited into a hacker controlled bank account which could be access online or through International ATM machines.

Most companies allow and encourage the use of direct deposit for paychecks and accounts receivable transactions.
These transactions utilize the ACH network. If the company uses an outside payroll company or accounting firm they very likely use an outside company to handle all ACH transfers. These ACH transfer companies are the targets for hackers. If a hacker can gain access to an ACH processing company, they can change the database to reflect a new bank account for a client. This will

cause all transfers normally sent to the victim's bank account to be re-routed to the new bank account controlled by the hacker/carder. If the new account is a corporate account, the bank has 72 hours to clear the transaction. After 72 hours, any discrepancies are the responsibility of the bank. In essence, a re-route of an ACH transfer for one week could bankrupt a company.

Identity Theft - When a hacker/carder steals personal data from any location, this information can be used to create fake id's, known as novelty id's to hackers, credit cards, bank accounts, loans and numerous other fraudulent media. If a hacker obtains a Social Security Number (SSN), they can use that information to apply for credit cards online in the real name of the SSN holder. They can also open bank accounts online at sites such as NetBank.com. These bank accounts will have credit cards or debit charges associated with them which can be sent via a re-mailer, trans-shipper or U.S. based associate to the hacker/carder's location.

A notable trend has been the use of stolen credit cards to buy access to information sites such as ConsumerInfo, ChoicePoint or Lexus/Nexus. From these sites the hackers/carders can identify addresses and telephone numbers for cardholders whose cards were stolen but the full cardholder information was not obtained. These sites and the information provided by them have enabled hackers/carders to commit identity theft at will.

Fake Sites - Similar to the fake store sites detailed above, hackers/carder will create fake auction, escrow and bank sites. As stated above the three possibilities for these shops are: the product is not shipped and the card is not charged, the product is not shipped and the card is charged or the product is shipped and the card is charged.

If the product is not shipped and the card is not charged, the hacker is simply collecting cards to use later. Often times the customer will forget about the purchase or will not worry about the lack of receipt because their card was never charged.

If the product is not shipped and the card is charged, the hacker was just stealing the money and will have to re-establish the fake site under a different name after approximately 6 weeks. The customer will often complain in these cases resulting in a chargeback to the fake sites merchant account. When the chargeback is not paid, the merchant account will be shut down and the hacker will start afresh.

If the product is sent and the card is charged, then the hackers have coupled their schemes. Meaning they are using one of the other schemes to obtain products to then sell on their site. The stolen goods will be shipped to the unsuspecting customer per the deal, but the hacker/carder will now have the customer's credit card. If the hacker/carder is patient and waits three to six months before making a charge, it will be nearly impossible for the customer to determine from which site the card was stolen. The added bonus is, if the original retailer of the re-sold goods reported the serial numbers of the equipment as stolen, when the new customer tries to register the equipment, it will red-flag the customer. By the time the transactions are sorted out, the hackers/carders and their site will be long gone with the money from the sale of stolen merchandise.

Extortion – When all other methods have been exhausted, many of which have been successful, hackers and carders will turn to basic extortion to obtain money. The most common extortion is phrased similar to the following:

"Hello, I have found holes in your system, for $2000 dollars I will fix the holes and make sure no other hackers gain access to your system. I would hate to have to tell your customers about you lack of security."

This threat usually comes in the form of an email or fax. If the victim does not respond, a second email and/or will be sent stating if the victim does not pay, the extortionist will be forced to post the stolen information on the Internet.

The interesting thing about extortion is often two or more members of the group responsible for the intrusion and theft will try to extort the same company independently. This results in confusion for the victim and the extortionist.

DDOS – Distributed Denial of Service (DDOS) attacks are not often considered part of profit making but recent trends show the use of DDOS attacks are being used in association with extortion. Once hackers have created a BotNet through the use of tainted (files/programs containing a virus/worm payload as well as IRC client with instruction to call home periodically) viruses, file sharing downloads (warez, mp3s, etc.) or straight hacking, DDOS attacks will be launched knocking particular sites offline for days at a time. (Those sites on the same network as the targeted site will suffer a loss of service as well making them collateral damage and future extortion victims.) Victims will often pay

extortionists the requested sum rather than suffer the loss of business. Some enterprising individuals, known as botmasters, who have successfully build large botnets, will hire themselves out. They are in essence cyber mercenaries willing to DDOS any and all sites if the price is right.

Collecting the Money

Once all the fraud is committed and the profits have been reaped, the hackers and carders need to convert the money to cash. The most common request is to have the money wired via Western Union (WU). For a small percent of the profit, WU clerks in Eastern Europe will look the other way if the recipients' Id does not match the name of the individual retrieving the cash. If a passphrase is used, there is no need for an Id. Finally, WU transfers can be used to fund ATM cards, which then require no Id's and no personal contact to obtain the funds.

All of the schemes allow the hackers and carders to convert the money into electronic credit that must be sent to a bank account or e-currency repository. These repositories can be as simple as an online bank account such as NetBank and INGDirect or normal bank accounts at banks that have less stringent banking requirements, i.e., off shore banks in Latvia, the Republic of Nauru or Cyprus.

The problem with these methods is the paper trail associated with keeping money in a bank.

With the advent of e-currency/online escrow accounts, came the advent of e-currency ATM cards, also known as pre-paid credit/debit cards. These cards can be purchased for a small fee and funded using any of the e-currencies currently available including, EVOCash, Egold, LogixPay, eBullion, GoldMoney, Pecunix and NetPay. The cards are in essence pre-paid ATM cards that are funded by sending money to the particular e-currency broker. The cash is then withdrawn at any ATM that accepts the respective ATM cards.

Providers of prepaid Debit cards or e-Currency ATM cards include, SwiftPay, WMcards, Ecount, Wired Plastic, Green Card, Citi Cash Card, Eufora, as well cards issued by the e-currency companies and hundreds of others.

Many enterprising subjects have set themselves up as middleman for the carders. These individuals set up online

businesses that handle the money-laundering and stolen property sales ("consignment shops") aspects of the schemes for the carders. The sites will offer bank accounts, debit cards and drop addresses to the carders in exchange for a fee. The carders will then have the profits from extortions, Paypal fraud, Auction fraud or any of the other schemes deposited into the account or shipped to the address. However, no real bank account will be set up for the carders. The site owner will open one bank account and using an Excel type spreadsheet, assign accounts to each of his clients. When money is deposited into the bank account of the site owner, a special denotation will be required indicating into which client account the money is to be deposited. This denotation will mean nothing to the legitimate bank at which the site owner's account resides. The site owner will deduct his percentage and denote the remaining amount on his spreadsheet as belonging to the specified client. The client can then have this money transferred to a bank account, a pre-paid debit card or use the money to purchase e-currency. Basically, the site owner has created their own bank without the regulations or oversight of a legitimate bank.

Conclusion

An organized use of the above detailed schemes could result in the de-stabilization of the banks and the credit card industry being victimized. These schemes have already been attributed to the collapse of several businesses and were utilized to finance at least one terrorist attack (the Bali bombing). At a minimum the loss, which exceeds $10 billion a year in fraud and damage to computer networks, can being blamed for the rise of purchase prices to consumers and the rise of interest rates on credit cards.

International financially motivated hackers are talented, educated and willing to do anything for money. They do not fear law enforcement because they think they cannot be caught. They do fear the FBI but only if they come to the United States. They are overseas therefore they are invincible. However, plans are being made to work with the respective law enforcement agency in each of the countries where hackers and carders have been identified. The intention of these cooperative efforts is to provide law enforcement with the proper training to catch the hackers and carders, to arrange their prosecution either in their home countries or in the U.S. and to obtain copies of their computer hard drives for use against additional targets.

This cooperation has already worked in Belarus, England, Canada and has been requested by Turkey, Ukraine and Russia.

Finally, these hackers/carders offer up information regarding hacking and carding freely online. Thus far, all indications are the schemes are being used by loosely connected groups who join force for one or two jobs and then part ways. Given the availability of the information and the changing climate of the world, in the near future, these attacks/schemes will be operated by highly organized groups with various political agendas. Online chatter has begun regarding “big hits” such as attacking various countries’ central banks, shutting down systems and bilking large corporations for millions of dollars. All indications are this type of crime will continue unfettered if law enforcement does not increase our knowledge base and cooperate internationally.

Though we will never stop this type of crime, by understanding what they are doing and how they are profiting, we may be able to limit the criminal’s effectiveness while dissuading others from trying to hack and card in the first place.