THE ULTIMATE BEGINNER AND ADVANCED GUIDE TO CARDING ONLINE

BY BAILOPAN

BAILOPAN@EXPLOIT.IM

INTRODUCTION

Fraud is something I have been doing for many years, even before internet fraud was a thing. So it is safe to say I have a vast knowledge and experience in this business. I have written this tutorial with the intention of helping beginners and even advanced fraudsters take their operations to the absolute next level. I have included most if not all of my knowledge from this part of the business in this guide. For many of you who have read my previous tutorials, I'm sure you are already familiar with my tendency to go much in-depth over everything and I plan on keeping that same level of quality on this tutorial as well. This guide is amazing for advanced fraudsters who want to make a lot more money. Beginners who are just starting out in the online fraud business will also find this guide extremely helpful to kickstart their journey as many of the things I will go over are used every single day during different fraud operations and will be valid for many years to come. I recommend you DO NOT skip any chapters of this guide, even if you are already familiar with the topic being discussed. Every chapter has its own equal importance and skipping chapters are for lazy people who do not want to learn. If you do not learn in this business, you WILL fail. Success requires patience and perseverance so keep that in mind.

FRAUD DICTIONARY

FULLZ: This is someone's entire data cluster and it's what is used to create bank drop accounts, and for setting up payment processors on fake online stores. This could also be used for many different things such as conducting an ATO (Account-Take-Over) on someone's bank account, opening new lines of credit under their name, and much more. Fullz are extremely valuable information to us and in fact a NECESSITY to be able to open bank drops. Fullz usually comprise of Background Checks, Credit Reports, Credit Scores, Full Names, Addresses, Social Security Number (SSN), Date of Birth (DOB), Driver's License Numbers, and more.

CVV: This can either be someone's full credit card details, or someone's full debit card details. CVV is simply a fraud slang for credit/debit card details, there's not much to it. We can use these details to "card" information on someone online, such as background or credit reports that can be used for various purposes such as opening bank drops and conducting an ATO (Account-Take-Over) on the victim's bank account, or we can use these CVV details to order physical/digital products that will be sent to a drop address.

CVV DUMPS: A credit card dump, is an unauthorized digital copy of all the information contained in the magnetic strip of an active credit card, created with the intention of illegally making a fake credit card that can be used by cybercriminals to make purchases. Credit card dumps are used by fraudsters to capture valuable card data such as the card number and expiration date. These can be obtained in a number of ways. The most popular method nowadays is "skimming", a process in which an illegal card reader is used to copy the data from a credit card. Other methods include hacking into a retailer's network or when a malware-infected point-of-sale device is unwittingly used by a retailer, sending the information to the criminals.

DUMPS SERVICE CODE: Many fraudsters think that there are only 2 types of dumps, 101 and 201. The truth is there are many other types of dumps. Carders usually work with either 101 or 201 but the majority will prefer 101. This is known as the SERVICE CODE of a dump. The service code contains 3 characters and you can find a dump service code just by looking at a dump, regardless of the fact if it has both TRACK1+TRACK2 or just TRACK2. Example, let's say we're looking at the dump 4256 746500930321=1402101700102054. The service code of this dump is 101, which is located right after the expiration date of the card, which in this case is 1402 (FEB 2014). The value of the service code determines where the cards are suitable to be used and in what way. Below is a detailed explanation of each service code available today.

First digit (usage variables):
- 1xx: Worldwide use, usually doesn't have a smart chip.

- 2xx: Worldwide use, does have a smart chip and required to use smart chip if the card reader reads the chip
- 5xx: National use, a list of regions can be allowed by the bank (often called region locks).
- 6xx: National use, a list of regions can be allowed by the bank but required to use smart chip if the card reader reads the chip
- 7xx: Only useable according to what has been agreed with the bank

Second digit (authorization)
- x0x: Normal authorization, normal usage.
- x2x: Contact issuing bank.
- x4x: Contact issuing bank, exceptions rules by bank.

Third digit (services that the card can be used for):
- xx0: Can be used for anything, require PIN.
- xx1: Can be used for anything without PIN.
- xx2: Can be used to buy goods or pay a service, cannot retrieve cash, PIN not required.
- xx3: ATM only ,PIN required.
- xx4: Cash only, PIN not required.
- xx5: Can be used to buy goods or pay a service, cannot retrieve cash. PIN required
- xx6: No restrictions to use, will ask for PIN when possible.
- xx7: Can be used to buy goods or pay a service, cannot retrieve cash. PIN required when possible.

TRACK1+TRACK2 DATA: There are up to three tracks on magnetic cards known as tracks 1, 2, and 3. Track 3 is virtually unused by the major worldwide networks, and often isn't even physically present on the card by virtue of a narrower magnetic stripe. Point-of-sale card readers almost always read track 1, or track 2, and sometimes both, in case one track is unreadable. The minimum cardholder account information needed to complete a transaction is present on both tracks. Track 1 has a higher bit density, is the only track that may contain alphabetic text,

and hence is the only track that contains the cardholder's name. The information on track 1 on financial cards is contained in several formats that goes from A to M. The "A" is only used by the bank itself, so we do not need to pay much attention to it. The "B" is where the holder's financial information is stored, the most important section of the magnetic stripe. C to M, is used for the ANSI Subcommittee X3B10, and N to Z is the information that is available for use of individual card issuers. This is how the track 1 looks like.

%B5XXXXXXXXXXXXXX2^GEORGENULL/MAX^1103101000000001000000003000000?;

- % for Start Sentinel
- B for Bank Type Credit Card
- 5XXXXXXXXXXXXXX2 is the Primary Account Number, which in most cases is the number printed on the front of the card, but not always.
- ^ is the separator
- GEORGENULL is the card holder's last name
- / is the separator
- MAX is the card holder's first name
- ^ another separator
- 11 expiration year, 03 expiration month
- 101 SERVICE CODE
- 00000000100000000003000000 is the discretionary data
- ? is the end

So now that you've seen the information that is stored in track 1 and the letter containers, you should have already figured out that credit card dumps are mainly the first 2 tracks.

Track 2 data is used by ATMs, physical payment processors and in any online website. There are a lot of components in this track, the layout is shown below.

| START SENTINEL | PRIMARY ACCOUNT NUMBER | FIELD SEPARATOR | ADDITIONAL DATA | END SENTINEL | LONGITUDE REDUNDANCY CHECK |

With a more in-depth examination of the data, you can see how a credit card number and holder's main information is stored into the track 2 data.

5XXXXXXXXXXXXXX2=1103200XXXX00000000?* ^^ ^^ ^ ^ ^^ ||_ CARD NUMBER || | |_ ENCRYPTED||_ LRC |_ START SENTINEL|| | PIN*** |_ END SENTINEL || |_ SERVICE CODE FIELD SEPARATOR _||_ EXPIRATION
Now let's break it down.

- ; : Start Sentinel
- 5XXXXXXXXXXXXXX2: Primary account number, the PAN. This would be the credit card number you always see printed on the front of the plastic.
- 1103: Expiry Date. Always year first then month.
- 200: Service code.
- XXXX00000000: Discretionary data, which includes the PIN verification, the card verification value and the last 3 digits on the back of the card aka the CSC/CVV2 code.
- ?: The End Sentinel
- With ^^ ^^ ^ ^ ^^ begins the track 3 data, which as said previously is completely useless.

Most carders and hackers, will only seek out the TR1 and TR2 data. That's where the term CVV dumps comes from.

WEB/ONLINE WALLETS: This is a program or web service that allows users to store and control their online shopping information, like logins, passwords, shipping address and credit card/bank details, in one central place. It also provides a convenient and technologically quick method for consumers to purchase products from any person or store across the globe. Such examples of web wallets are PayPal, Google Wallet, and Venmo. We can use such wallets for many purposes that will be discussed in further guides.

SKIMMER: This is a device made to be affixed to the mouth of an ATM and secretly swipe credit and debit card information when bank customers slip their cards into the machines to pull out money. Skimmers have been around for years, of course, but fraudsters are constantly improving them. Card skimming accounts for more than 80 percent of ATM fraud. Some sophisticated skimmers are even able to transmit stolen data via text message.

EMBOSSER: A device that stamps the cards to produce the raised lettering where the CVV holder's name is, card number, etc…

TIPPER: A device that adds the gold/silver accents to the embossed characters.

MSR (MAGNETIC STRIPE READER/WRITER): Used by fraudsters to write dumps into actual physical blank cards or gift cards (and driver's licenses, student IDs, etc..). If you want to use blank white cards, you will need a printer for the card template, embosser and tipper, which can be pretty expensive, however it is worth it if you know how to correctly use these things.

POS (POINT-OF-SALE) SYSTEM: This is the time and place where a retail transaction is completed. At the point of sale, the merchant calculates the amount owed by the customer, indicates that amount, may prepare an invoice for the customer (which may be a cash register printout), and indicates the options for the customer to make payment. It is also the point at which a customer makes a payment to the merchant in exchange for goods or after provision of a service. After receiving payment, the merchant may issue a receipt for the transaction.

ACH: This stands for Automated Clearing House, which is an electronic network for financial transactions in the United States. ACH processes large volumes of credit and debit transactions in batches. ACH credit transfers include direct deposit, payroll and vendor payments. Moving money and information from one bank account to another is done through Direct Deposit or via ACH transactions, credit or debit. This is used a lot by fraudsters to siphon money out of the bank accounts of unsuspecting victims, which is extremely easy.

PAYMENT PROCESSORS: A payment processor is a company (often a third party) appointed by a merchant to handle transactions from various channels such as credit cards and debit cards for merchant acquiring banks. They are usually broken down into two types: front-end and back-end. Front-end processors have connections to various card associations and supply authorization and settlement services to the merchant banks' merchants. Back-end processors accept settlements from front-end processors and, via The Federal Reserve Bank for example, move the money from the issuing bank to the merchant bank. In an operation that will usually take a few seconds, the payment processor will both check the details received by forwarding them to the respective card's issuing bank or card association for verification, and also carry out a series of anti-fraud measures against the transaction. Additional paraments, including the card's country of issue and its previous payment history, are also used to gauge the probability of the transaction being approved. Once the payment processor has received confirmation that the credit card details have been verified, the information will be relayed back via the payment gateway to the merchant, who will then complete the payment transaction. If verification is denied by the card association, the payment processor will relay the information to the merchant, who will then decline the transaction. Such examples of payment processors are Square, PayPal, Stripe and Flint

PAYMENT GATEWAYS: This is a merchant service provided by an e-commerce website that authorizes credit card or direct payments processing for e-businesses, online retailers, or traditional brick and mortar stores. The payment gateway may be provided by a bank to its customers but can be provided by a specialized financial service provider as a separate service. It facilitates a payment transaction by the transfer of information between a payment portal (such as a website, mobile phone or interactive voice response service) and the front-end processor or acquiring bank. Here's how a typical transaction plays out.

1. A customer places an order on a website by pressing the “Submit Order” or equivalent button, or perhaps enters their card details using an automatic phone answering service.
2. If the order is via a website, the customer’s web browser encrypts the information to be sent between the browser and the merchant’s webserver. In between other methods, this may be done via SSL encryption. The payment gateway may allot transaction data to be sent directly from the customer’s browser to the gateway, bypassing the merchant’s systems. This reduces the merchant’s Payment Card Industry Data Security Standard compliance obligations without redirecting the customer away from the website.
3. The merchant then forwards the transaction details to their payment gateway.
4. The payment gateway converts the message from XML to ISO 8583 or a variant message format and then forwards the transaction information to the payment processor used by the merchant’s acquiring bank.
5. The payment processor forwards the transaction information to the card association (e.g. Visa/Mastercard/AMEX). If an American Express or Discover Card was used, then the card association also acts as the issuing bank and directly provides a response of approved or declined to the payment gateway. Otherwise, the card association routes the transaction to the correct card issuing bank.
6. The credit card issuing bank receives the authorization request, verifies the credit or debit available and then sends a response back to the processor with a response code (approved or denied). In addition to communicating the fate of the authorization request, the response code is also used to define the reason why the transaction failed (e.g. insufficient funds, or bank link not available). Meanwhile, the credit card issuer holds an authorization associated with that merchant and consumer for the approved amount. This can impact the consumer’s ability to spend further (because it reduces the line of credit available or it puts a hold on a portion of the funds in a debit account).
7. The processor forwards the authorization response to the payment gateway.

8. The payment gateway receives the response, and forwards it on to the website (or whatever interface was used to process the payment) where it is interpreted as a relevant response then relayed back to the merchant and cardholder. This is known as the Authorization or “Auth”
9. This entire process typically takes 2-3 seconds.

WEB DOMAIN: This is traditionally known as the name or URL of a website and is sometimes called the host name. The host name is a more memorable name to stand in for the numeric, and hard to remember, IP address of a website. This allows the website visitors to find and return to a web page more easily. It also allows advertisers the ability to give a website a memorable name that visitors will remember and come to, hopefully leading to conversions for the web page. The flexibility of website domains allows several IP addresses to be linked to the same website domain, thus giving a website several different pages while remaining at the easily remembered address.

VIRTUAL CARDING: This is the process of purchasing physical or digital goods online using someone else’s credit/debit card details.

PHYSICAL CARDING: This is the process of purchasing physical goods by going to an actual physical store in-person and using pre-made credit cards with dumps punched in them to conduct the fraudulent transactions. Transactions are also possible to be conducted with an Android phone using NFC payments with TR1+TR2 data.

CARDING: Term used when referring to using someone else’s CVV details to conduct a fraudulent purchase on an online website or physically in person in a store using DUMPS. Example, we can CARD a cellphone using someone else’s details through Amazon, or CARD a $400 belt at a Gucci Store using dumps that were punched into a blank card using devices specifically made for such purposes.

CARD HOLDER: The owner of the CVV that we’re using to conduct the fraudulent transaction.

BILLING ADDRESS: An address directly attached to a CVV. This is where the card holder's bank sends his bills, hence the name BILLING.

SHIPPING/MAILING ADDRESS: An address used exclusively to receive mail. Most websites do not allow transactions to be accepted if the billing address on a credit card and the shipping address provided to the website are different.

AVS & NON-AVS: AVS stands for Address Verification System. This is a system used to verify the address of a person claiming to own a credit card. The system will check the billing address of the credit card provided by the user with the address on file at the credit card company. AVS is used by mostly all merchants in the US, Canada, and UK. Because AVS only verifies the numeric portion of the address, certain anomalies like apartment numbers can cause false declines; however, it is reported to be a rare occurrence. AVS verifies the numeric portions of a cardholder's billing address. For example, if the address is 101 Main Street, Highland, CA 92346, United States, AVS will check 101 and 92346. Cardholders may receive false negatives, or partial declines for AVS from e-commerce verification systems, which may require manual overrides, voice authorization, or reprogramming of the AVS entries by the card issuing bank. Cardholders with a bank that does not support AVS may receive an error from Internet stores due to lack of data. All countries besides UK, US & Canada, are NON-AVS.

VBV & NON-VBV: This is an XML-based protocol designed to be an additional security layer for online credit and debit card transactions. VBV stands for Verified by Visa. This is used to validate the card holder's identity and prevent fraudulent transactions. It works by asking for additional information either from the card holder directly or by analyzing data behind the scenes to see if the purchase fits the usual payment behavior. When a website and a card have Verified by Visa, a message box pops up on screen after you have entered the Visa card details. You are then asked to identify yourself with your Verified by Visa password or a code sent to your phone. What you need to do at this stage varies but your bank will tell you about the method they use and what they expect from you. If you don't notice

the VBV message box appearing but instead see a revolving wheel, all the security associated with VBV is still happening but in the background. And you don't need to do anything. The bank is verifying the purchase by making background checks to see that everything is at it should be. Any Visa card that does not have the above feature in place, is known as NON-VBV and you should ultimately look for NON-VBV cards instead of VBV, because as you can see this verification process is a huge hassle.

MASTERCARD SECURECODE (MCSC): MasterCard SecureCode is very much similar to Visa's VBV. It is a private code for a MasterCard account that gives the card holder an additional layer of online shopping security. Only the card holder and the financial institution know what the code is, merchants are not able to see it. Fortunately, the majority of MasterCard cards do not have this security in place.

AMERICAN EXPRESS SAFEKEY: This is one of the least used security measures around, and it is not even available in the United States. However, it is the same thing as MasterCard SecureCode and Visa's VBV.

NEAR-FIELD COMMUNICATION (NFC): NFC technology lets smartphones and other enabled devices communicate with other devices containing an NFC tag. It is widely used as a payment method, all you have to do is swipe your smartphone at the checkout in any store, and most stores support NFC. Apple Pay for example, uses NFC.

SSN: Social Security Number. This is a nine-digit number issued to U.S. citizens, permanent residents, and temporary (working) residents in the United States. Although its primary purpose is to track individuals for Social Security purposes, the Social Security number has become the national identification number for taxation and other purposes. SSN is frequently used by those involved in identity theft, since it is interconnected with many other forms of identification, and because people asking for it treat as an authenticator. Financial institutions generally require an SSN to set up bank accounts, credit cards, and loans-partly because they assume that no one except the person it was issued to knows it.

MMN: Mother's Maiden Name. This is the name of someone's mother BEFORE they got married, that is, her name with her original family name (or "surname"), the name she used when she was a girl and a young woman. "Maiden" here means "unmarried woman". So "maiden name" refers to a woman's name when she was still an unmarried woman. In many cultures, when a woman gets married, she takes the family name of her husband's family, so her name changes. Example, let us say your mother's name was Mary and she was born into the Smith family. Her maiden name would be "Mary Smith". Then, let us say, she married your father, whose name was Tom Jones. When she married him, she became Mary Jones. That is her married name, but her maiden name will always be Mary Smith. This is one of the most important aspects to conducting successful transactions online for high value products, as most banks ask this as a security question for making any changes to the account.

DOB: Date of Birth. This is one of the most important pieces of information you can get on your victim. The reason for that because with the date of birth, full name and hometown, you can easily find the person's SSN. And also because you need this information if the bank ever asks you for it.

MAIL DROP: A mail drop is a location where you are able to freely receive illegal products that were either carded, or drugs. You never want to use your own house for these purposes as it will bring a lot of headache for you in the future. With a mail drop, you can use it let's say a month, and never show your face there again. This will make extremely hard for any law enforcement official to track you down and arrest you or conduct an investigation into your life.

BIN: Bank Identification Number. This is the first four to six numbers that appear on a credit card. The bank identification number uniquely identifies the institution issuing the card. The BIN is key in the process of matching transactions to the issuer of the charge card. This numbering system also applies to charge cards, gift cards, debit cards, prepaid cards and even electronic benefit cards. This numbering system helps identify identity theft or potential security breaches by comparing

data, such as the address of the institution issuing the card and the address of the cardholder. The first digit of the BIN specifies the Major Industry Identifier, such as airline, banking or travel, and the next five digits specify the issuing institution or bank. For example, the MII for a Visa credit card starts with a 4. The BIN helps merchants evaluate and assess their payment card transactions. After submitting the first four to six digits of the card, the online retailer can detect which institution issued the customer's card, the card brand (such as Visa or MasterCard), the card level (such as corporate or platinum), the card type (such as debit card or a credit card), and the issuing bank country. BINs can be check through the websites below.

- https://www.bincodes.com/bin-checker/
- http://binchecker.com/
- https://bincheck.org/
- https://binlists.com/

PROXY SERVER: Every time you reach out to a website or connect with anyone online, your online connection gives your computer "address" to the site/person you're connecting with. This is so that the other end knows how to send information back to your computer. That address is your public IP address. IP stands for Internet Protocol and you can check yours by going to whoer.net. Without an IP address, you wouldn't be able to do any Internet/online activity and others online wouldn't be able to reach you. It is how you connect to the world. Your IP address comes from your Internet Service Provider (ISP). Unfortunately, there are a lot of privacy concerns when it comes to public IP addresses such as

- Your IP address identifies where you are in the world, sometimes to the street level.
- It can be used by websites to block you from accessing their content.
- It ultimately ties your name and home address to your IP address, because someone is paying for an Internet connection at a specific location.

A proxy lets you go online under a different IP address identity. You don't change your Internet provider; you simply get a proxy server. A proxy server is a computer on the web that redirects your web browsing activity. Here's what that means.

- Normally, when you type in a website name (Amazon.com or any other), your Internet Service Provider (ISP) makes the request for you and connects you with the destination-and reveals your real IP address, as mentioned before.
- When you use a proxy, your online requests get rerouted.
- While using a proxy, your Internet request goes from your computer to your ISP as usual, but then gets sent to the proxy server, and then to the website/destination. Along the way, the proxy uses the IP address you chose in your setup, masking your real IP address.

Proxy servers are commonly used by identity thieves to fake their location to the cardholder's billing address. The reason for that is because some websites will not allow a transaction to be accepted, if the purchase is being made from a location much farther away than the cardholder's billing address.

BANK DROPS: Bank drops are bank accounts that are opened specifically for the purpose of storing your dirty funds. Once you open them, you can decide whether you wish to withdraw the funds directly from the account as cash by going to the bank ATM, or possibly clean them with specific methods, and only after cleaning them, cashing them out (my preferred method and much safer). It is important to mention also, that all bank drop accounts, are opened ONLY with the information of someone else (aka FULLZ), so there is absolutely no possibility of these dirty funds ever being traced back to your real identity. To open one of these bank drop accounts, you will usually require the person's DOB + SSN + DL + BACKGROUND CHECK + FULL CREDIT REPORT + MVR/DRIVING RECORD for maximum success.

PROXY SCORE: When it comes to fraud detection, finding proxies is a big topic. Fraud detection begins with thinking intelligently about the IP address associated with a transaction. Where is that IP address, and how does that location relate to other transaction data? Whereas most IP addresses inspire confidence, those associated with a proxy generate suspicion. As the name suggests, a proxy acts as an intermediary, passing requests from one computer to other servers. But although there are legitimate uses of proxies, fraudsters are well known to use proxies. Detecting proxies comes with two challenges. The first is how to recognize an IP address as a proxy. The second is how to distinguish a "good" proxy from a "bad" one; since by definition, a proxy is merely an intermediary, a proxy is not high risk in and of itself. To consider how best to address these challenges, it's helpful to look to the primary goal of ecommerce fraud detection: thinking intelligently about the IP address associated with a transaction in order to assess risk. Fraud detection uses transaction data as the basis for this thinking and risk assessment. Using this data and analysis, they're able to gain insight into the kind of traffic on a particular IP address. The Proxy Score, is a summary of risk associated with an IP address. You want this to be as low as possible (0.80 MAX). Anything above 0.80, you should move on and look for another proxy as that will lead to a declined transaction 70-80% of the time. You can check your proxy score on the websites below. Ideally you want the lowest proxy score that you can find, I have used RDPs with a proxy score of 0.01 many times.

- https://getipintel.net/
- https://www.maxmind.com/en/request-service-trial?service_minfraud=1 (FREE TRIAL)
- xdedicvhnguh5s6k.onion (private RDP provider website, but the best one to check this kind of stuff, send me a PM and I will send you an invite)

FRAUD SCORE: Every online transaction is given what is called a "Fraud Score". This is a number ranging between 0 and 999. It gives the merchant a number from which he can determine if a given transaction is fraudulent or not. Transactions that are given high fraud scores (over 300), are placed under manual verification by an agent, who will decide if they contact the cardholder or let it through. Scores

over 500 with auto-decline, will block the card and an agent will immediately contact the cardholder. Some banks have different criterias but certain things that can affect the fraud score are:

- Comparison with the usual spending pattern of the cardholder
- Location of the charge
- Amount
- Risk factor associated with the merchant

For example, a $15.56 charge in the cardholder's local Walmart will not trigger anything, while a purchase of $2000 on Newegg will have an extremely high fraud score and probably auto-decline if the cardholder rarely makes purchases online.

RISK SCORE: This is a percentage given to each transaction that ranges from 0.00% to 100.00%. The factors that determine this score are whether an IP address, email, device and proxy used are high risk or low risk. This is determined by fraud systems that websites have in place such as MaxMind, which establishes the reputations of IP addresses, emails, geolocation and other parameters. This should always be checked before purchasing an RDP. Anything above 1.00% will lead to declined transactions most of the time.

MAC ADDRESS: Whether you work in a wired network, or a wireless one, one thing is common for both environments. It takes both network software and hardware (cables, routers, etc.) to transfer data from your computer to another-or from a computer thousands of miles away to yours. In the end, to get the data you want right to YOU, it comes down to addresses. So not surprisingly, along with an IP address, there's also a hardware address. Typically, it is tied to a key connection device in your computer called the network interface card, or NIC. The NIC is essentially a computer circuit card that makes it possible for your computer to connect to a network. An NIC turns data into an electrical signal that can be transmitted over the network.

Every NIC has a hardware address that's known as a MAC, for Media Access Control. Where IP addresses are associated with TCP/IP (networking software), MAC addresses are linked to the hardware of network adapters. A MAC address is given to a network adapter when it is manufactured. It is hardwired or hard-coded onto your computer's network interface card (NIC) and is unique to it.

Unfortunately, a MAC address can be used by law enforcement in combination with Internet Service Providers, to find someone's true location and consequently his identity. Further in this guide I will explain how to mitigate this risk.

VIRTUAL PRIVATE NETWORK (VPN): An essential step of conducting a successful fraudulent transaction, is having a VPN. Most of you already know what this is, but for those of you who don't, VPNs are used to funnel your entire traffic to an encrypted tunnel. This way, none of your traffic is able to be captured by your ISP or an attacker, and consequently sniffed upon. Nor can your real location be revealed if you are using a good and reliable VPN that prevents DNS leaks. This will be discussed in more detail further in this guide.

RDP: Remote Desktop Protocol. This is a protocol developed my Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. You can for example, be using a Linux machine, and connect to a Windows 7 RDP. RDPs are absolutely essential to conducting a successful fraudulent transaction, especially HACKED RESIDENTIAL RDPs. The reason for that is because these RDPs are from a REAL PERSON, with a REAL LOCATION/IP, and REAL COMPUTER and BROWSER FINGERPRINT. They will exponentially increase your success rate. They will also be discussed in more detail further in this guide.

SOCKS5: This is a proxy server that allows us to fake our real location. This is very good if let's say, we have a credit card with a billing address in Miami, we can use a SOCKS5 near the billing address in Miami so that the website we are conducting the fraudulent transaction in doesn't raise our fraud score because the transaction

is being conducted in another state/far away from the credit card's billing address as this will lead to a declined transaction most of the time.

VIRTUAL MACHINE: This is an emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. They allow you to run an operating system using an app window on your desktop that behaves like a full, separate computer. The most used software for virtual machines are respectively, Virtual Box and VMWare. Unfortunately, they are not as reliable as using an RDP, but they are very good to CONNECT to an RDP, so as to leave no traces on your original computer. Windows and OS X are still not reliable enough in the aspect of leaving no traces, as the virtual machine in these operating systems, will leak information to the host OS, and consequently leave a lot of illegal evidence/traces on your computer that could later be used as potential evidence in an investigation. However, you should never let it get to that point the first place.

OPERATIONS SECURITY (OPSEC)

This is the most important aspect of being a successful fraudster. The reason for this is because there's no point in doing all of this, if we're going to eventually be caught, and have all of your assets seized by the government. Unfortunately, the United States doesn't take these things lightly, and they will do everything they can to persecute cybercriminals and put them in jail, which most of the time are given sentences of over 10 years in jail for minor offenses. They are the biggest and most powerful nation in the entire world, and their resources are absolutely endless. We MUST take every precaution possible to mitigate any of these risks and to make sure our hard work will never be taken from us by such governments. Even if you do not live in the United States, you should still very much worry about them as they are involved in pretty much every single international issue that occurs, especially in cybercrime cases.

I have written an extensive guide over 100 pages long on just the topic of OPSEC and creating your perfect fraud expert setup for maximum success, and security against such adversaries, of which I am currently selling for $25 ONLY for a limited time. If you are any serious about doing this business and following my guidance, I HIGHLY recommend you purchase my guide and follow each and every step outlined in it to secure yourself to the max. Remember, if you want to be a criminal, then do your homework, or don't be a criminal.

With that said, in this chapter I won't go into as much detail as my OPSEC guide goes, as there are many things to keep in mind and I wouldn't be able to fit everything into only one chapter, that's the reason I made a guide specifically for the purpose of explaining privacy and security. However, I will give you a perfect setup in this tutorial.

First of all, I want to introduce you to the absolute best operating system available today when it comes to security and privacy. It is called Qubes OS. This operating system allows us to run isolated environments. It is basically a giant virtual box. You can run different OSs in Qubes as different virtual machines. For example, we have a virtual machine for the Whonix OS, another for Fedora, Debian, and those are only the VMs that come pre-installed with the OS. You can install Kali Linux in Qubes, Windows, and all kinds of different OSs. If one of these VMs ever get compromised, we are fine. We simply delete the VM and create a new one. If you want to learn more about the Qubes OS, then navigate to the link below, it is full of tutorials and even videos about the OS so you can get a good look at what we'll be working with.

https://www.qubes-os.org/doc/

Qubes has a very small compatibility range and so will not work with most computers unfortunately. However, if you want to become truly a professional cyber-criminal, then I highly recommend you invest in a new computer. Don't be lazy or close-fisted with security, as that will lead to problems and much headache

for you in the future, trust me on that. Below are the laptops I recommend, from best (most expensive) to worst (cheapest). All of them work perfectly with the current Qubes 4.0. All of the prices were taken from Amazon at the time of this writing, so keep in mind, you may get cheaper, or more expensive.

LENOVO THINKPAD X1 CARBON 5TH GEN ($1845): This laptop is absolutely amazing, and if you have money to buy it, then do it. It's totally worth it, as it will last you for many years to come. This was voted the best business laptop at CES 2018. The performance of this laptop is absolutely incredible and will make your work incredibly smooth and easy. This is the laptop that I currently use and the one I recommend to all my clients on top of every other one.

LENOVO THINKPAD T460P ($1350): Also works perfectly with Qubes 4.0 and the performance is amazing. The one above is much better, but if you want to get this one instead and save some money, I'd say go ahead.

LENOVO THINKPAD T450S ($530): This laptop is also very good, although the performance of the above one is much better, this one does boast some impressive features. You can get it on Amazon for very cheap. It comes with i7 processor, 8GB RAM, 256GB SSD (you may want to upgrade the SSD). I have tested this computer with Qubes 4.0 and it also works perfectly and smooth.

LENOVO THINKPAD X230 ($235): This is a last resort type of laptop, and you should only get it if you're really low on money. The performance will be terrible, but definitely usable. Qubes 4.0 runs perfectly with it, and everything works exactly as it should, just really slow due to the old processor and low memory. If you're thinking of buying this laptop, keep in mind you will most likely need to upgrade some of the components to make it run smoothly.

BEST QUBES SETUP FOR FRAUDULENT ACTIVITIES

Having a perfect setup for your fraudulent activities, is one of the most important aspects of being successful in this business. If you have a bad setup, you will most

likely run into problems, and declined transactions on a daily basis. As I have explained previously in this guide, Qubes OS is the absolute best operating system for our purposes, and is the OS I use for my fraudulent activities, in fact it is THE ONLY ONE I use. Not only will Qubes protect you to the maximum extent possible, to ensure that LE can't successfully uncover your real identity, but to websites, you will look like just another shopper looking for something expensive to buy, which in turn will make us extremely successful. Below I will outline the perfect setup for Qubes OS. All of the setup outlined below is explained in much more detail on my OPSEC guide, so I would highly recommend you get that one as well.

- First, we will anonymize our MAC address by following this tutorial (https://www.qubes-os.org/doc/anonymizing-your-mac-address/) for our NetVM.
- Once we have fully anonymized our MAC address, we will route our NetVM to the FirewallVM. From there, we will route the traffic to the VPN VM.
- Now we need to setup our VPN VM to route all traffic to the VPN tunnel and restrict all non-VPN connections with iptables rules. If you are running Qubes 4.0, please follow this tutorial (https://github.com/tasket/Qubes-vpn-support). If you are on Qubes 3.2, follow this tutorial (https://www.reddit.com/r/Qubes/comments/6h4ue2/guide_setting_up_a_vpn_with_mullvad_on_qubes/). Feel free to send me a message if you run into any problems. Check everything is good and that there are no leaks in your connection by navigating to whoer.net and dnsleaktest.com and conducting tests. Even with webRTC enabled, you should have 0 leaks because of the iptables rules.
- Once we have setup our VPN VM, we will create another VPN VM and route our traffic to the 2nd VPN tunnel. This is extremely important, as it will add an amazing extra layer of security to your setup. You should use 2 different VPN providers. The ones I recommend are respectively from best to worst, NordVPN, TorGuard, and Mullvad. You should follow the same steps as the 1st VPN VM to create the 2nd. Check everything is good and that there are no leaks in your connection by navigating to whoer.net and dnsleaktest.com and

conducting tests. Even with webRTC enabled, you should have 0 leaks because of the iptables rules.

- From the 2nd VPN VM, we will send our traffic to our Tor network VM (usually called sys-whonix).
- In sys-whonix, we will edit the torrc configuration file and make sure we are using obfs4 bridges to connect to it. This will make much harder for anyone snooping on our traffic to see we are using Tor (although I seriously doubt anyone would be able to do so if you followed the steps above correctly). You can do that by following this tutorial (https://www.whonix.org/wiki/Bridges).
- Now that we have our network completely set up, we will move on to actually connecting to our RDP to conduct our work. To do that, simply create a new AppVM, name it whatever you so wish, use the Template WHONIX-WS for it, give it network access through sys-whonix, and open a new Terminal on it. Once you have done that, run the following command on that Terminal: sudo apt-get install remmina
- That command will install a program called “remmina” which will enable us to connect to our RDPs anonymously with the Tor network.
- For the RDP, I recommend you purchase a Windows 7 one from xDedic (if you don’t have an account there, send me a message and I will sell you an RDP from there, or you can also purchase an invite to the website from me if you so prefer, that way you won’t rely on me or anyone else to purchase your RDPs, you can simply login the website and purchase them yourself). xDedic is the best website for RDPs, and the reason for that is because they sell clean hacked RDPs, that belong to an actual real person, with a real digital fingerprint, and with a real IP/real location. The reason we want this is so that the website we are conducting our work in, doesn’t realize we are a fraudster and declines our transaction. I prefer not to use Socks5 as they are far from being reliable as RDPs are, and PLEASE, do not use a Socks5 in conjunction with one of these RDPs, as that would be dumb, and will mess up your entire setup.
- Once you have all of this setup, all you need to do is pick a website that you want to card, get a CVV close to the zip code of your RDP (some websites will

decline your transaction if you are placing an order too far away from the CVVs billing/shipping address) and work your magic! This “magic” will vary from website to website, and one thing you need to keep in mind is that most websites will require you to call the card holder’s bank using a burner spoofed to the card holder’s number to change his billing address. The reason for that is because as mentioned previously, websites in Canada, United States and United Kingdom, all have AVS systems in place that will check your billing address with the card holder’s bank. If you use a shipping address that differs from the billing address, especially a shipping address too far from the card holder’s address, you will get a declined transaction. You could still get approved if the shipping address you are using is not too far from the card holder’s billing address (anything 30-50 miles away is already too much), but it’s always better to call the bank and do a change of billing.

- If you are purchasing anything above $600 dollars, chances are you will need to conduct a what is known as an ATO on the card holder’s account. ATO stands for Account-Take-Over. This is a process in which you will call the bank, change the card holder’s phone number, then wait 5-7 days and call again to change his billing address, you can also add a temporary address if you prefer, which is much better in my opinion (Bank of America doesn’t allow temporary addresses unfortunately, Chase is the best one for this). The reason for this is because most websites will require you to put the card holder’s billing phone number on check out and for orders above $600, they will call the card holder to confirm the transaction. Not to mention that the bank may find all of this very suspicious, especially if the card holder hasn’t done a purchase as big as that in months and will ring them to confirm. And, there is also the possibility of the card holder having what is known as “text updates/alerts” for charges that big on his account. All of those things may lead to declined transaction, and a burnt card.
- I also recommend you use a .edu, .org or .gov email with the card holder’s name, to conduct such high value fraudulent transactions. This will significantly lower your fraud score and will help you a lot in getting approved.

- Make sure you act like a real shopper. Wait 2-3 days before purchasing and during that meantime, put products in your cart, look around the website, make it look LEGIT. Make it look like you care about how much you're spending, because people do care about that. If you register an account, and then right off the bat purchase a laptop worth $1500, you can't expect to be approved. I will further explain in detail all of this in this guide.

WINDOWS & MAC OS X VIRTUALBOX SETUP

I realize most people will not go as far as the setup above requires them. And although that is very unfortunate, it is a fact that I can't neglect. Below I will outline a good, but much more unsuccessful and unsafe setup. Unfortunately, OS X and Windows, are both closed-source operating systems, and particularly Windows, is full of zero-day exploits and vulnerabilities that are easily exploitable by law enforcement officials. Not to mention these OSs are full of NSA/FBI/CIA backdoors and are just not safe from a privacy standpoint, proceed with caution and most importantly, ATTENTION to detail. Do not skip any steps.

Now, when it comes to the Virtual Box setup, what you need to do is first of all, download Virtual Box obviously (https://www.virtualbox.org/wiki/Downloads), then download VeraCrypt (https://www.veracrypt.fr/en/Downloads.html) and create a hidden encrypted volume with at least 30GB of space, then mount that hidden encrypted volume. Then, download WinISO (http://www.winiso.com/download.html), and google "WinISO serial number" so that you are able to complete the next step. Next, download MagicISO (http://www.magiciso.com/download.htm), get a .iso of Windows 7 and burn it into a bootable media on a blank CD using WinISO. Then mount the .iso into the virtual drive using MagicISO.

Then, create a new virtual machine on Virtual Box and name it whatever you so wish. Go to settings and on "System" use at least 2GB RAM for the base memory. On boot order use HDD and CD/DVD. Then, go to storage and add your virtual drive letter where you mounted the .iso on Controller:IDE. On "Network", choose

NAT and refresh the MAC address (refresh every single time you boot the Machine). Then, install Windows 7 on the virtual machine.

Once you have done all that, move the .vdi files into the hidden encrypted VeraCrypt volume. Then, on the Windows 7 virtual machine install TMAC to change the MAC address every time you connect to the internet (https://technitium.com/tmac/), CCleaner, and Bleachbit to clean your cookies and temporary data.

Then every time you start the machine, go to the Windows 7 CMD, and type these commands:

ipconfig /release
ipconfig /renew
ipconfig /flushdns

Once you have completed all these steps, download the VPN of your choice and install it on your newly created virtual machine. You can also get another VPN and install it on your main OS, that way you have 2 VPNs for added security. I recommend 2 different providers, and make sure you use an anonymous email that can't be traced back to you, and only pay with clean BTCs.

From that virtual machine, connect to an RDP by going to the Start menu and typing "Remote Desktop" in the search box. When "Remote Desktop Connection" appears in the search results, click on it. Next, enter the IP address of the target computer and press connect. Enter the login credentials, click OK and you should be inside the RDP.

Now that you have your OPSEC set up, I will teach you about how to card successfully.

VIRTUAL CARDING

As I have mentioned previously in the fraud dictionary section of this guide, virtual carding is the process of purchasing physical or digital goods online using someone else's credit/debit card details. However, there is A LOT more to it. You can't simply get someone's CVV details and go on a shopping spree, that will not work and will only lead to burnt cards & declined transactions. There are many things you need to keep in mind and in this chapter I will go into detail on how exactly all of it works.

The main goal of a carder, is to cheat websites into thinking he's the legit owner of a CVV. This is the most important aspect of carding, because if you can't do that, nothing else will work. To be able to cheat the website, there are a couple of things we need to keep in mind.

- We need to use an extra clean hacked residential Windows 7 RDP (available on xDedic, again, if you don't have an account there just send me a message and we can work something out). Windows 7 is the 2nd most used operating system in existence today, right behind Windows 10 so that is why we are using it. We want to appear as generic as possible to the website, and never appear to be a "unique" user as that will raise our fraud score. A RESIDENTIAL RDP is essential, because it already has a digital fingerprint from a legit user, which will tell the website that we are a real person, from a real location, with a real computer, and not a fraudster using a proxy server in a virtual machine.
- We should either use Firefox or Chrome for fraudulent transactions inside of our hacked RDP. The reason for that is because again, we want to appear as generic as possible to the website, and those browsers are currently the most used browsers in existence. It is important to note that no changes should be done to those browsers, and no addons should be installed, you should use them AS THEY ARE BY DEFAULT.

- With Firefox or Chrome inside of your RDP, navigate to dnsleaktest.com and ipleak.net, then conduct tests to see if your real location is leaking. Then navigate to whoer.net and check your anonymity score, it should be 100%. Sometimes it won't be because of the time-zone difference between your IP location and the system time, if that happens then simply change the system time to match your IP location, and do a re-test, it should then say 100% in your score. You should do this every time you wish to conduct a fraudulent transaction.
- Now we get a CVV that is close to the CITY and STATE that our RDP is located in. Example, if we have an RDP located in MIAMI FL, we want a CVV from MIAMI FL. The level of the CVV you need to get will depend much on the value of the transaction that you want to conduct. A card that would be used to purchase movie tickets/food delivery online, is not the same card you would use to purchase a $1000 laptop. However, a card that can be used to purchase a $1000 laptop, would easily approve a small movie ticket/food delivery purchase transaction, but you would never use a card like that for such purposes unless you don't know what you're doing.
- If you are carding something worth $500 or more, you will need to get a free .edu email registered in the name of the CVV holder by navigating to the website http://home.cccapply.org and selecting Cuesta College from the drop-down menu (this changes from time to time so Cuesta may not work for you, if it doesn't just try other colleges and one of them should eventually work). From there you apply to the college, and for the Social Security Number (SSN) you navigate to http://fakenamegenerator.com/, select MALE/FEMALE and then hit GENERATE. This will generate a new identity, from that you just need the SSN which will look something like this 427-70-XXXX. Just substitute the XXXX for any numbers and that should do fine. Fill out all the rest with the fake info (phone, address, etc…), just provide the correct sex. If you have his SSN, then you can use that as well and it will be a HUGE plus. For the email, you can use disroot.org, navigate to their website, create a new account with the CVV holder's name and use it for registering for the college. You will soon receive on that email your newly created @.my.smccd.edu email address details.

- If the .edu email method doesn't seem to be working for you, then you can simply card a domain with ipage.com and use a .org email that the domain provider will let you generate. You can also generate as many .org emails as you wish with your domain, just make the domain name something legit such as https://nmnenterprises.org or https://pierceandassociates.com/. To card the domain, follow the same steps outlined above and register with the domain provider with a yahoo email in the name of the CVV holder.
- Once you got the email ready, then you are finally ready to conduct the fraudulent transaction. Navigate to the website you want to card. If you are carding something worth $200 or more, then you should first create an account on the website using the .edu/.org email, browse the website to look like a real buyer, wait 2 days and browse the website during those 2 days for at least 30-40 min looking at products, putting stuff in your cart, etc… After you have done that, you can go ahead and proceed with the transaction.
- Keep in mind that as I mentioned previously, some websites will not accept transactions in which the billing and shipping addresses are too far away from each other (30 miles is already too much). If you get a card with a billing address less than 30 miles from your drop address, then you are very very lucky and you can proceed. If not, you will need to call the bank using a spoofed burner number (spoof to the CVV holder's number) and ask them to add a temporary shipping address/add an additional billing address to the account. They should be able to do that for you, unless it's Bank of America, I've run into problems before doing that with BoA. They will require you to change the billing address entirely.
- For the burner phone, it is entirely up to you to either purchase a phone for $40 dollars at somewhere like Wal-Mart or go to Amazon and purchase a phone like this (https://www.amazon.com/Phone-4-5mm-Ultra-Pocket-Black/dp/B00JN82EFO) which you can use for a month, and destroy it completely when done with carding for a few websites/CVVs. For the SIM card, you can go to T-Mobile and ask them for the $30 monthly plan (make sure you show them your phone so that they give you the right SIM card and ALWAYS pay with cash, you can even go a step further and use a hoodie when going to the store to mitigate the threat of cameras).

- To spoof your phone number, you can use the service https://www.spoofmyphone.com/ they allow you to pay with BTC and are very reliable.
- Before buying your RDP, ALWAYS check its PROXY, RISK, and FRAUD score. You can check all of that through the xDedic website (if you don't have an account there contact me and we can work something out).

CVV

There are a lot of websites nowadays on the web that will sell you stolen CVV. However, the problem with these websites is that they will most of the time, sell you CVVs that are either dead, or that are complete shit. I know this from my own personal experience with these websites, so I have completely given up on them. The only one I can currently recommend under good conscience is Yale Lodge (https://yalelodge.cm/), however, the registration to it is closed at the moment, and I have spoken to the owner, he is not currently selling registrations, but will very soon for 300-400 dollars (that money will be added to your balance on the website). So, if you want to purchase the registration, keep checking the website.

I am an experienced hacker, and I have taken advantage of flaws in website security systems many times to hack their databases. With that said, I currently have in my possession over 70k CVV and over 50k dumps for sale from different online databases. I check my CVVs for validity every single time before sending them out to my buyers, so you can be safe you will get valid cards from me.

To check out the balance of a card and check its validity, you can simply call the bank to which the card belongs to using your burner phone. Let's say it's Chase, you call Chase bank and use the automated prompt by typing your CVV number and its zip code. From there the automated prompt will tell you the balance of the card, its credit access line, amount in pending transaction authorizations, and recent transactions. You should take note of the 8 most recent transactions in case you need it. It is also good to know the CVV holder's spending patterns so we can mimic it. This will make things look much less suspicious to the bank.

CARDING LEVELS

When it comes to carding, there are 3 different levels to it. They are each outlined and explained below.

LEVEL 1 CARDING: This is the entry point for most carders, it includes such things as ordering pizza, movie tickets, and small purchases below $50. This is considered very easy carding and you will usually just require the CVV details, along with the full billing address of the CVV.

LEVEL 2 CARDING: This would be intermediate carding, and includes such things as carding background reports, credit reports, or physical products with a value below $200. For this you will require the same details as LEVEL 1 CARDING. However, it will vary depending on the website you are carding. Different websites have different security measures in place to curb fraudulent transactions and will require specific strategies.

LEVEL 3 CARDING: This is advanced carding, and not recommended for beginners. Things that fall under this category are for example, high value physical products above $400 in value, and everything on high security websites such as Amazon, Newegg, TigerDirect, etc... All of these websites will require you to perform an ATO (Account-Take-Over) on the CVV holder's account. This will require you to have the CVV details, full billing address, along with the victim's DOB, MMN, SSN, and background report. For this it is always good to get as much information as you can on the victim, as we will have to call the bank and perform changes in the holder's account to take over. This will be explained in much detail further in this guide.

CVV LEVELS

As mentioned previously in this guide, different cards are used for different purposes. You would never use a Signature Visa, with a credit access line of $30,000 to card movie tickets or pizza. Below I will outline all the card levels in existence today. It is important to mention, that for high value purchases you should ALWAYS look for CREDIT CARDS. Debit Cards are not good for making these high value purchases online. However, they could still have many uses such as purchasing background reports, credit reports, and all purchases below $200.

CLASSIC – Classic cards are recognized and accepted by a large number of merchants all over the world, including the Internet. This card is usually used by students, young couples, or people trying to establish credit. The limits of these cards are usually around $1000.

GOLD – A premium card used by people around the world. With higher spending limits and greater purchasing power, the Visa Gold card is the choice of consumers who want more from their cards. Average limit of this type of card is $3000.

PLATINUM – Platinum is one of the best cards around. Average limit could be around $8000.

BUSINESS – Very high limits, often around $15,000

CORPORATE – This is used by large corporations. The limits are usually around $15,000 as well.

SIGNATURE – The 2nd best card around. I've gotten many signature cards with a limit of $30,000.

PREMIER – Same as Signature. Limits are usually $30,000.

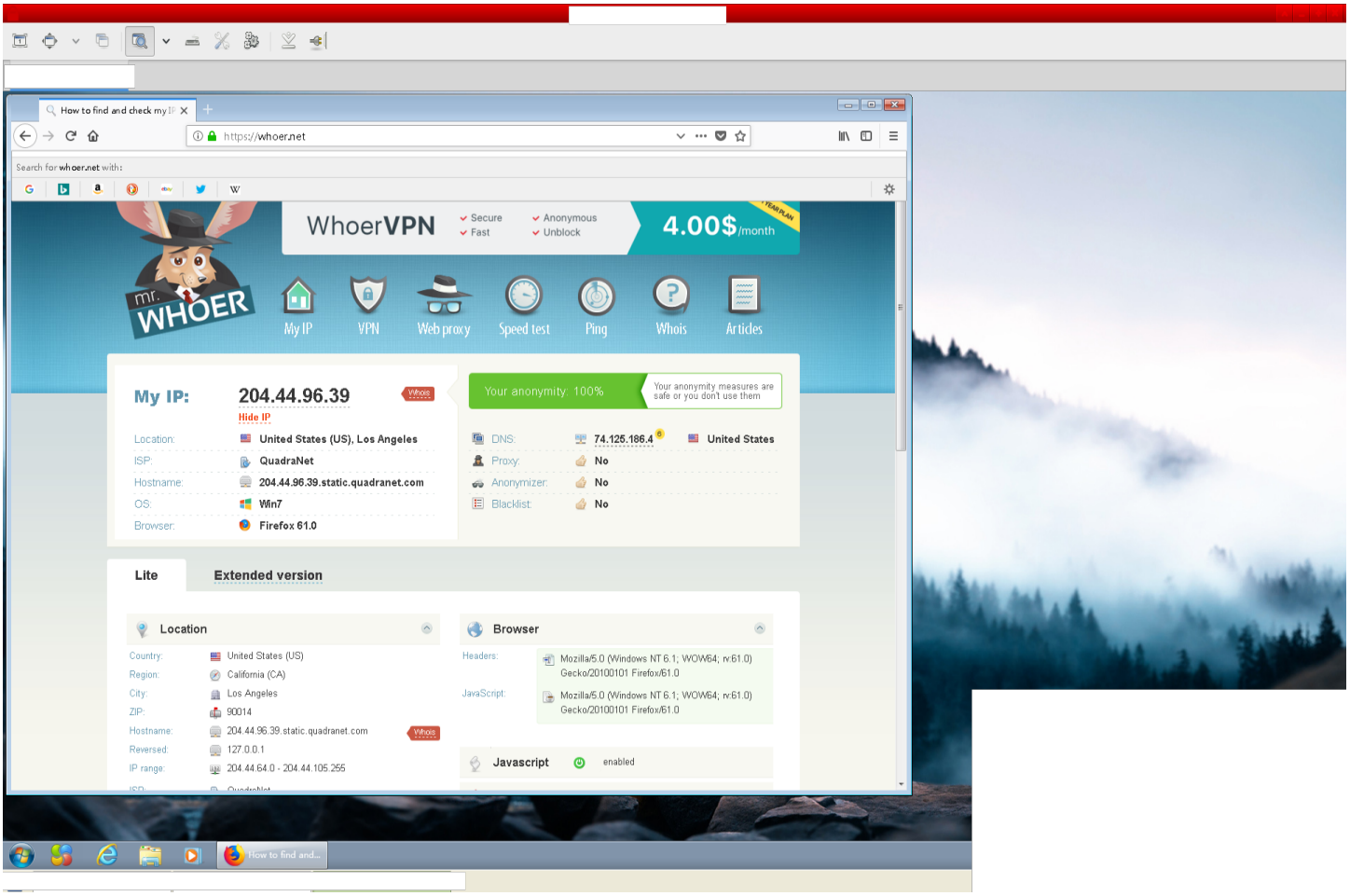
INFINITE – This is the absolutely best card around. However, it is incredibly hard to find. If you do manage to get your hands on one of these, you are very lucky. There are usually no limits to such cards.

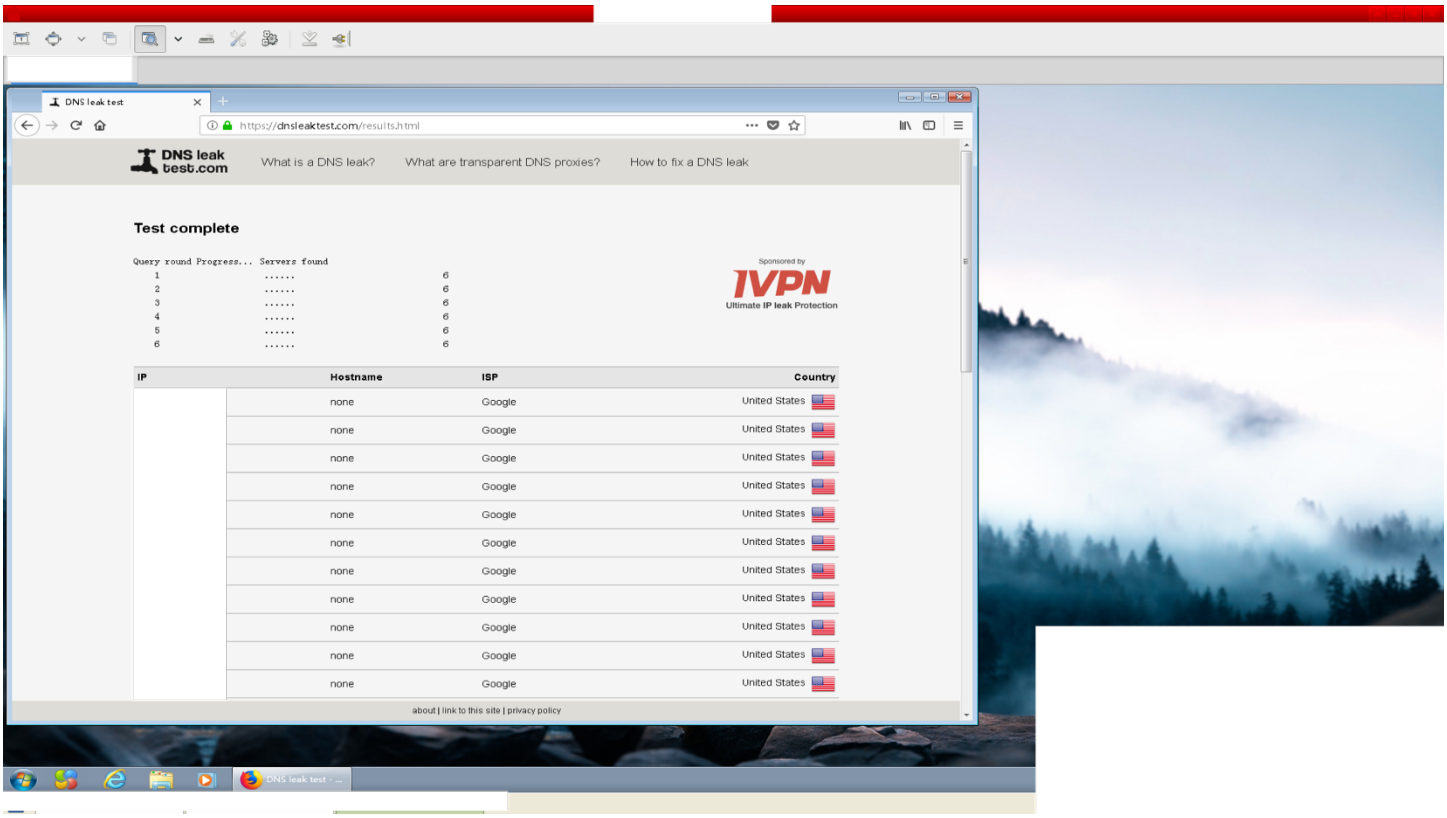
It is important to note that all these numbers are subject to change depending on the subject's credit score, history, and spending pattern.

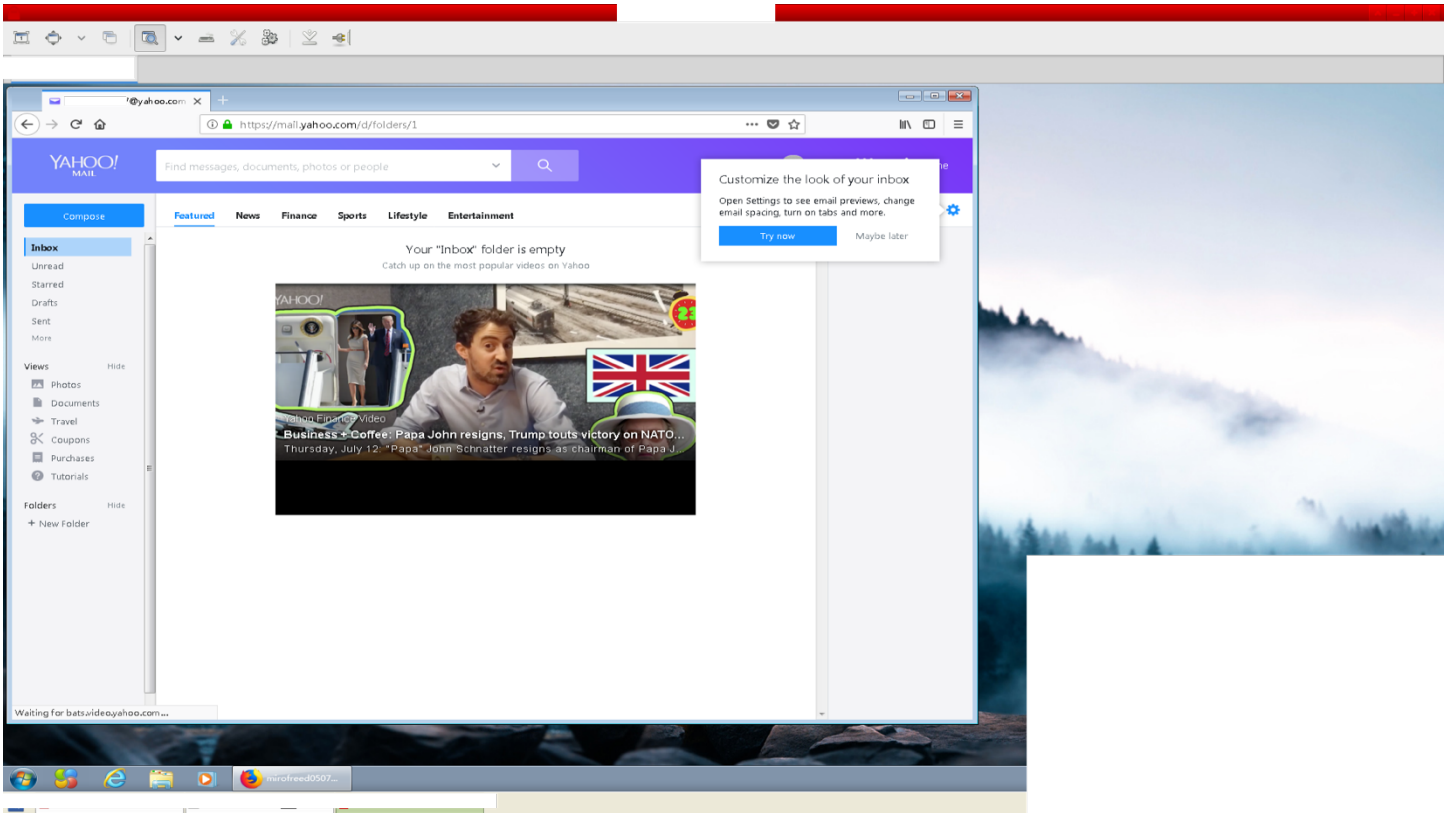
LEVEL 1 CARDING EXAMPLE

As previously mentioned in this guide, LEVEL 1 CARDING includes things such as ordering food online, buying movie tickets, and carding products below $50 in value. In this chapter, I will show you the process I go through when conducting a level 1 transaction. For this, I will be carding 2 movie tickets on the website https://www.fandango.com/.

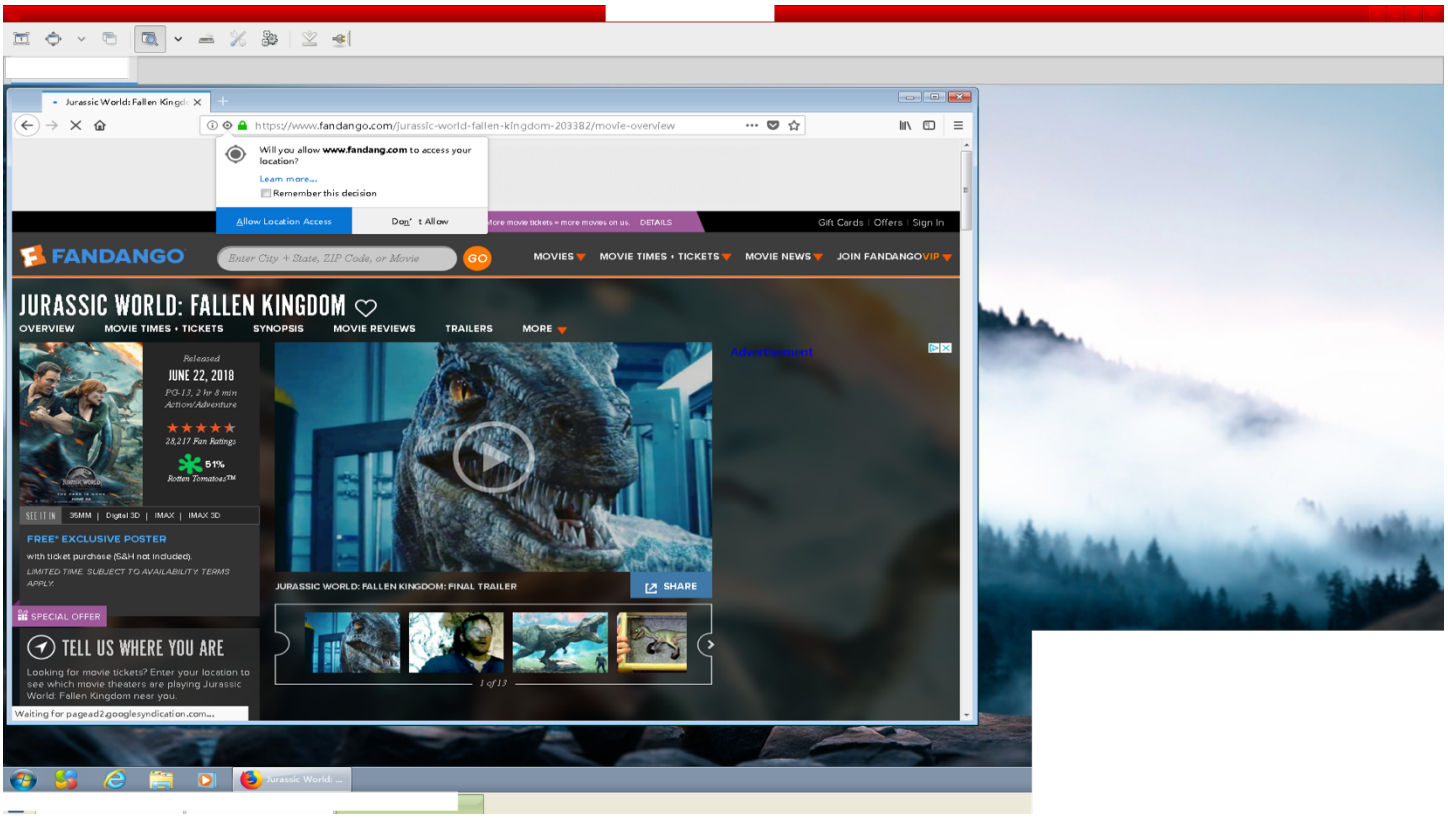
1. First of all, we will head to the Yahoo mail website to create a new email in the name of the CVV holder. Please note I am already inside the clean hacked Residential RDP close to the CVV holder's address at this point. And I have checked my setup on whoer.net and dnsleaktest.com as instructed (some parts of the images have been blurred out to protect my privacy). Zoom in the pictures if you need to do so.



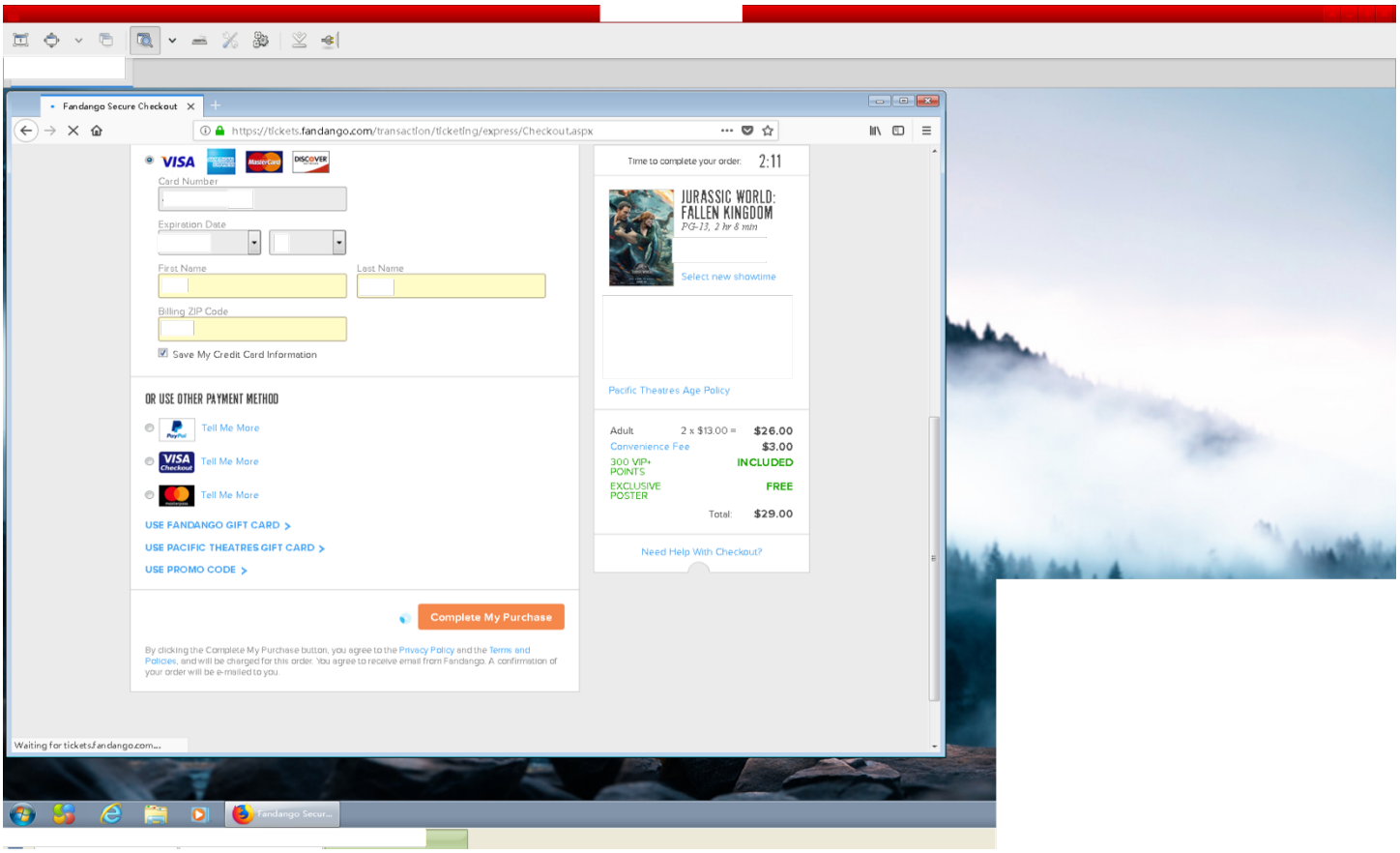

DNS leak test
https://dnsleaktest.com/results.html
DNS leak test.com
What is a DNS leak?
What are transparent DNS proxies?
How to fix a DNS leak
Test complete
Query round Progress... Servers found
1 6
2 6
3 6
4 6
5 6
6 6
Sponsored by
IVPN
Ultimate IP leak Protection
IP
Hostname
ISP
Country
none Google United States
about | link to this site | privacy policy


https://mail.yahoo.com/d/folders/1
YAHOO! MAIL
Find messages, documents, photos or people
Compose
Featured
News
Finance
Sports
Lifestyle
Entertainment
Inbox
Unread
Starred
Drafts
Sent
More
Views
Photos
Documents
Travel
Coupons
Purchases
Tutorials
Folders
New Folder
Your "Inbox" folder is empty
Catch up on the most popular videos on Yahoo
Customize the look of your inbox
Open Settings to see email previews, change email spacing, turn on tabs and more.
Try now
Maybe later
Business + Coffee: Papa John resigns, Trump touts victory on NATO...
Thursday, July 12: "Papa" John Schnatter resigns as chairman of Papa J...
Waiting for bats.video.yahoo.com...

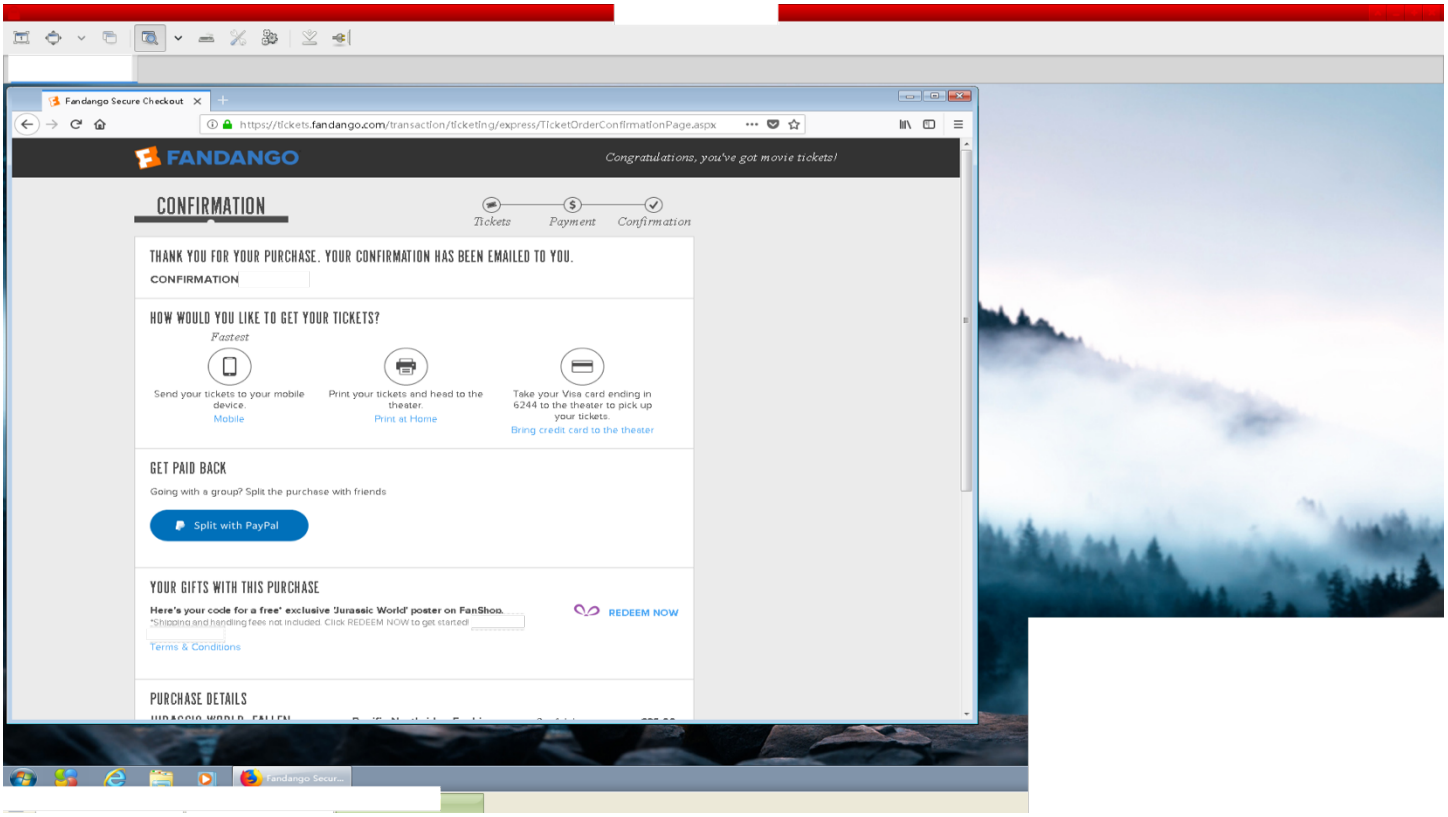
2. Now we will head over to the https://www.fandango.com/ website to get our tickets. Make sure you “allow location” on the browser. The rest is pretty straightforward, just look for tickets for the particular movie that you want on the ZIP that you want to watch it at and go to checkout.



3. Once we're at the checkout, we need to complete the transaction within 7 minutes (fandango has a timer as you can see on the picture). Make sure you DO NOT copy and paste the CVV details, type them like you would as a normal buyer. Same for the name, expiration date and all other details. By the way, for this specific transaction I used a VISA CLASSIC CREDIT CARD.



4. As you can see, my transaction has been successful, and so should yours! If you get a declined transaction, you did something wrong. Go back, retrace your steps and check where you slipped. If you were successful, have a great time at the movies!

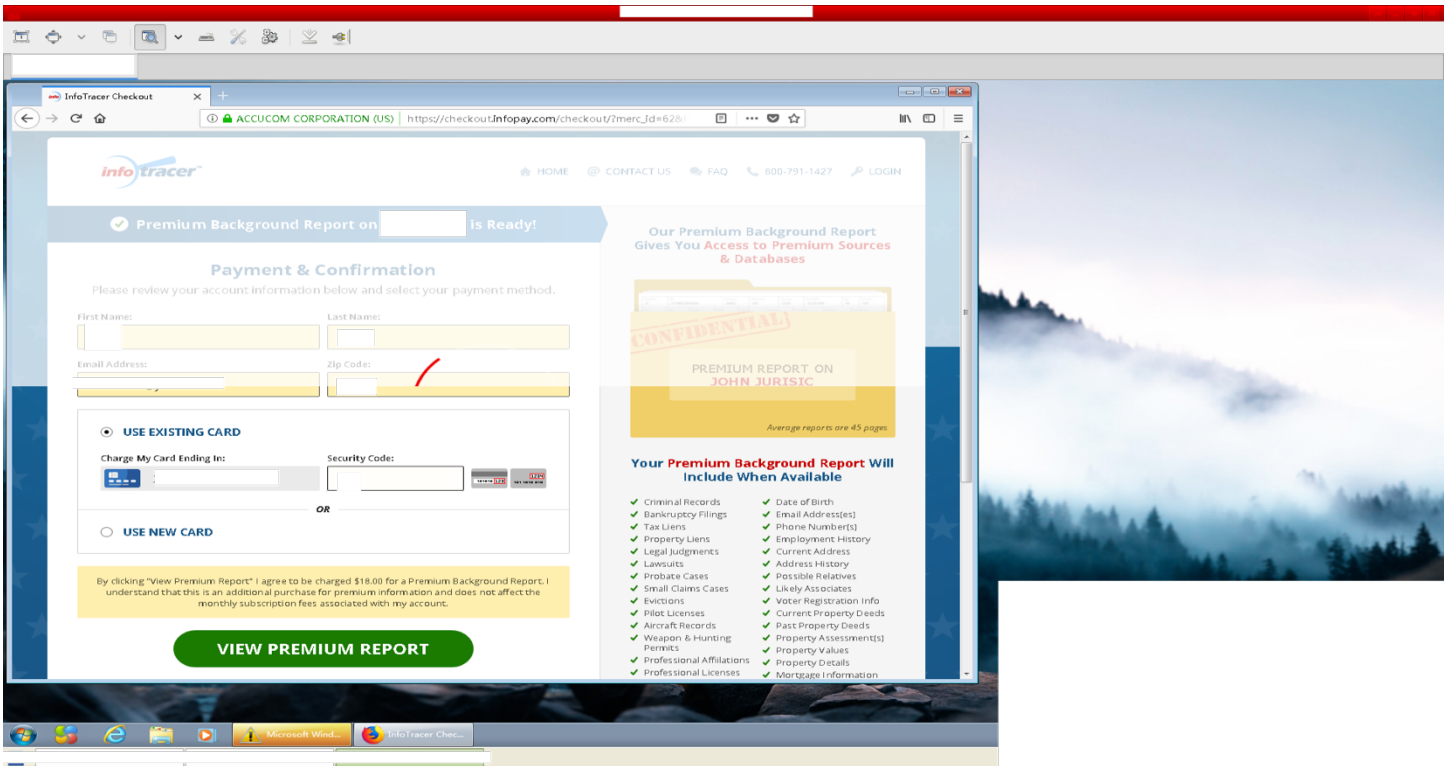


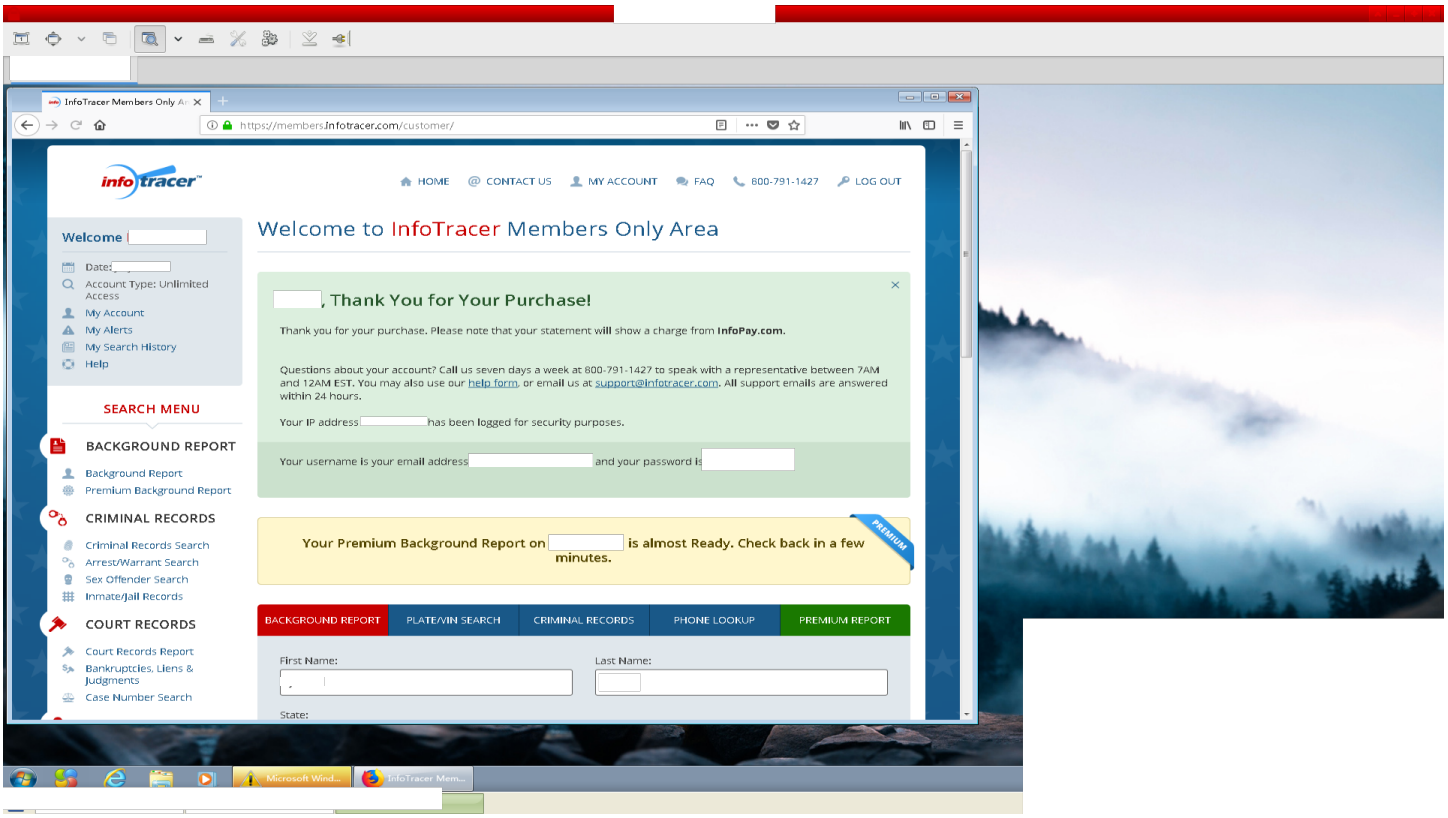
LEVEL 2 CARDING EXAMPLE

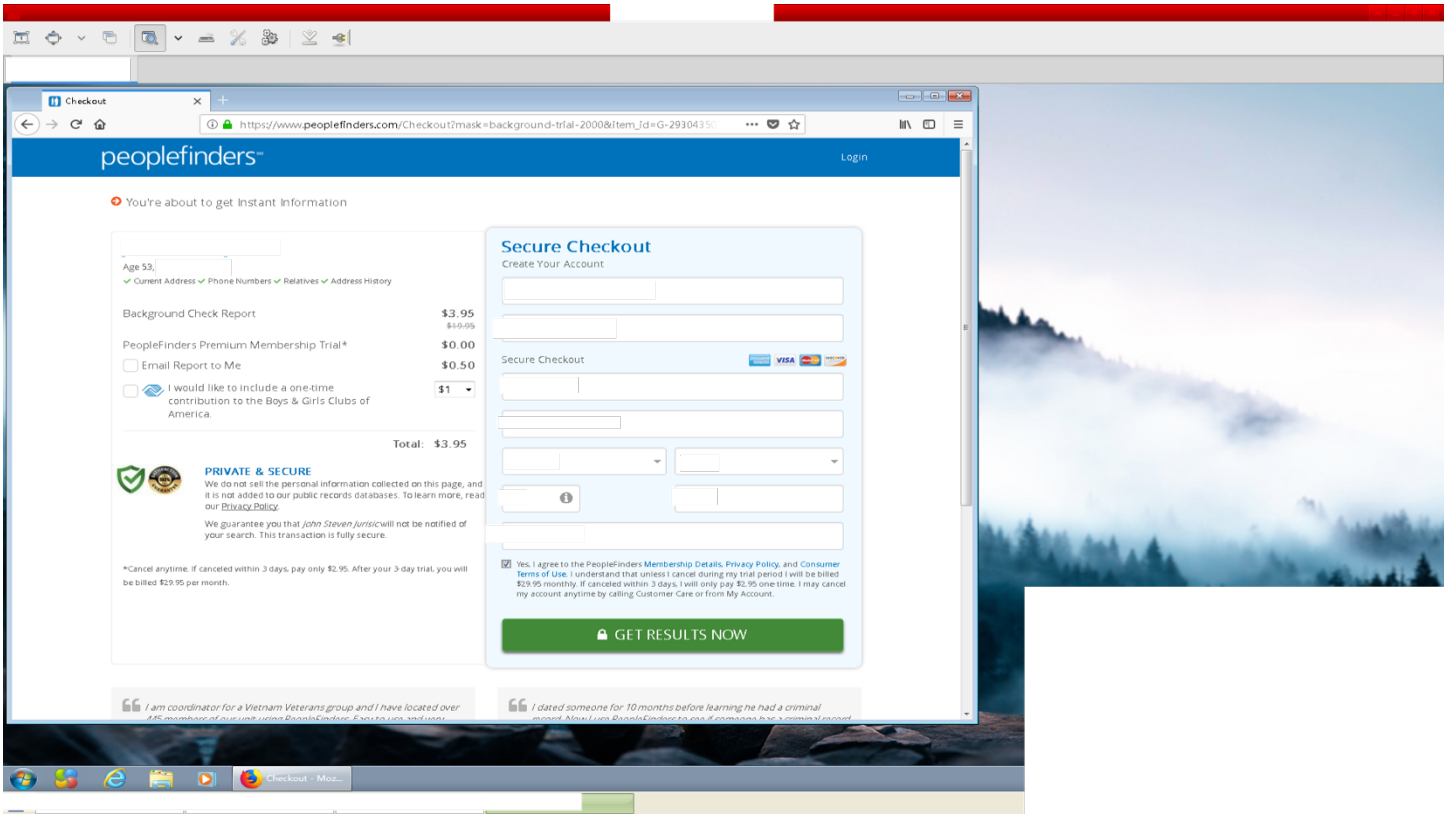
Now that we have got the basics out of the way, we can move on to LEVEL 2 CARDING, which as mentioned previously involves such things as carding background reports, credit reports, and physical products in the $100-$200-dollar range. In this tutorial, I will be demonstrating 2 successful BACKGROUND REPORT transactions, and a $100-dollar successful transaction at the website https://www.jcrew.com/. Again, some parts of the images were blurred out to protect my privacy.

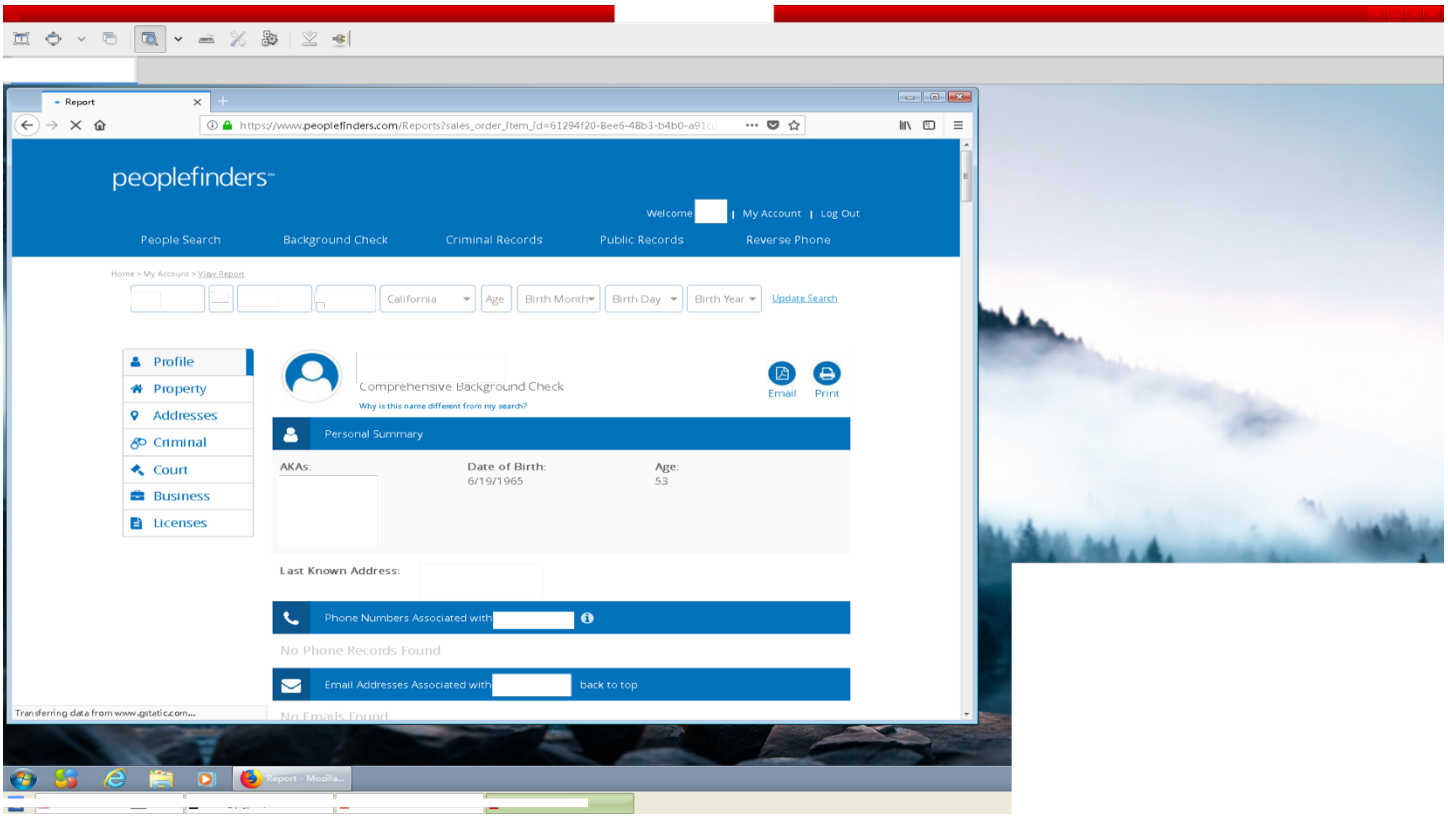
1. We're going to start with the background report. So, first of all we will check our setup by going to whoer.net and dnsleaktest.com and conducting the tests as instructed previously.

2. Once that is out of the way, we will navigate to the website we want to card the background report in. In my case this website is https://www.peoplefinders.com/ and https://www.infotracer.com/. Next, we will search for our target's name and buy his background report.

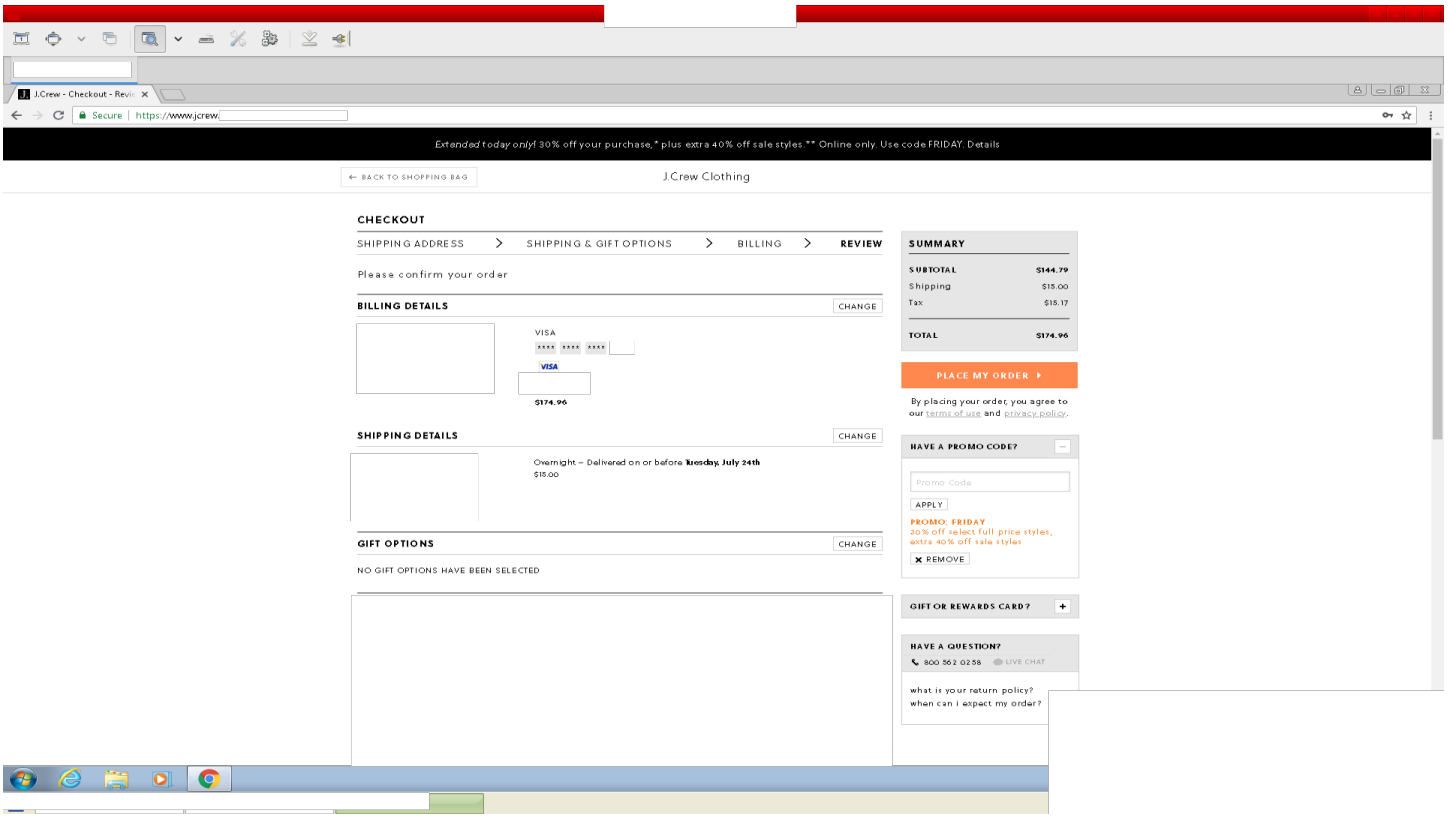


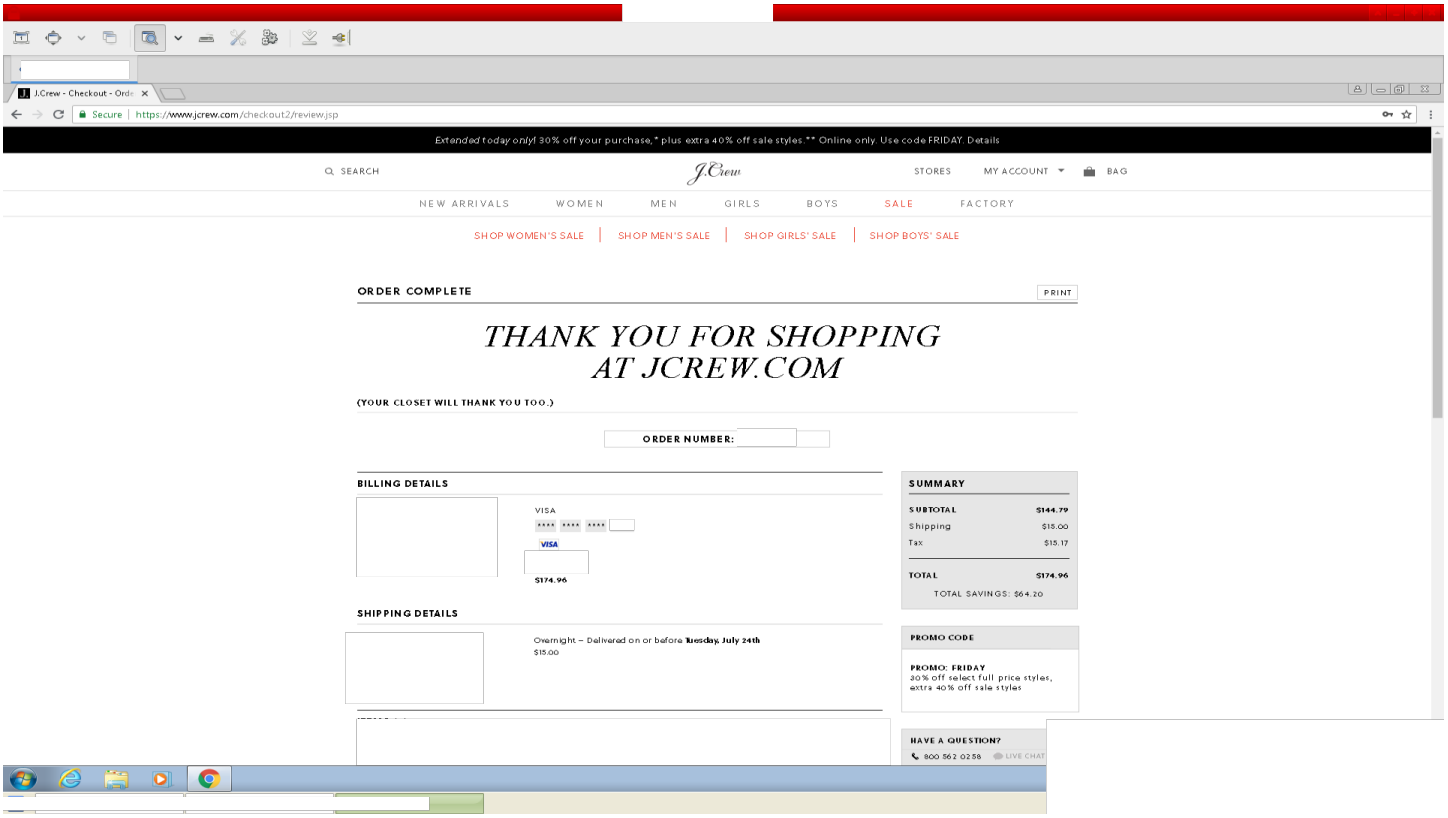

InfoTracer Members Only Ar
https://members.infotracer.com/customer/
infotracer
HOME
CONTACT US
MY ACCOUNT
FAQ
800-791-1427
LOG OUT
Welcome
Date:
Account Type: Unlimited Access
My Account
My Alerts
My Search History
Help
SEARCH MENU
BACKGROUND REPORT
Background Report
Premium Background Report
CRIMINAL RECORDS
Criminal Records Search
Arrest/Warrant Search
Sex Offender Search
Inmate/Jail Records
COURT RECORDS
Court Records Report
Bankruptcies, Liens & Judgments
Case Number Search
Welcome to InfoTracer Members Only Area
, Thank You for Your Purchase!
Thank you for your purchase. Please note that your statement will show a charge from InfoPay.com.
Questions about your account? Call us seven days a week at 800-791-1427 to speak with a representative between 7AM and 12AM EST. You may also use our help form, or email us at support@infotracer.com. All support emails are answered within 24 hours.
Your IP address has been logged for security purposes.
Your username is your email address and your password is
Your Premium Background Report on is almost Ready. Check back in a few minutes.
PREMIUM
BACKGROUND REPORT
PLATE/VIN SEARCH
CRIMINAL RECORDS
PHONE LOOKUP
PREMIUM REPORT
First Name:
Last Name:
State:

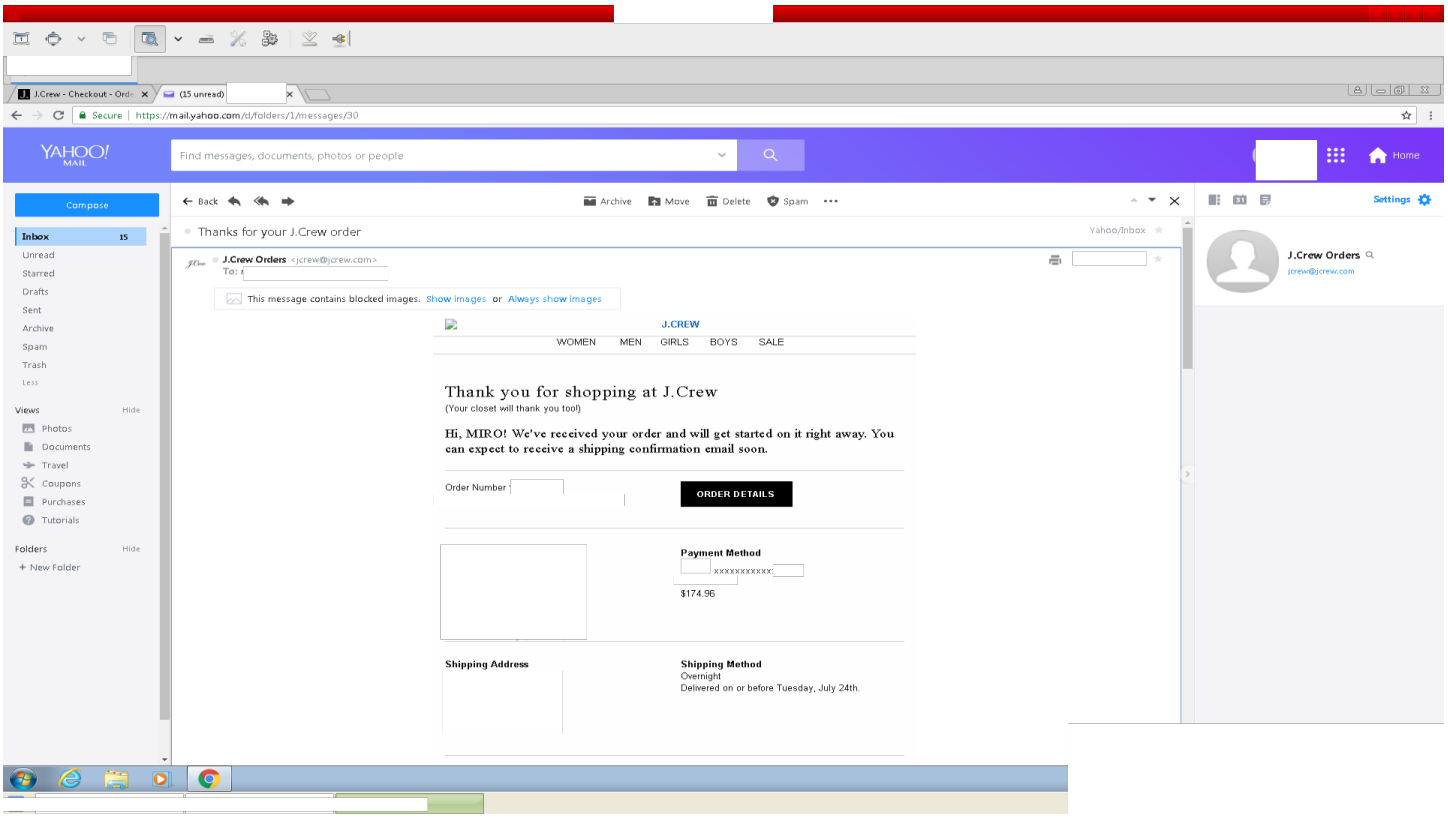

Checkout
https://www.peoplefinders.com/Checkout?mask=background-trial-2000&item_id=G-2930435
peoplefinders
Login
You're about to get instant information
Age 53,
Current Address Phone Numbers Relatives Address History
Background Check Report
$3.95
$10.05
PeopleFinders Premium Membership Trial*
$0.00
Email Report to Me
$0.50
I would like to include a one-time contribution to the Boys & Girls Clubs of America.
$1
Total: $3.95
PRIVATE & SECURE
We do not sell the personal information collected on this page, and it is not added to our public records databases. To learn more, read our Privacy Policy.
We guarantee you that John Steven Jurisic will not be notified of your search. This transaction is fully secure.
*Cancel anytime. If canceled within 3 days, pay only $2.95. After your 3 day trial, you will be billed $29.95 per month.
Secure Checkout
Create Your Account
Secure Checkout
Yes, I agree to the PeopleFinders Membership Details, Privacy Policy, and Consumer Terms of Use. I understand that unless I cancel during my trial period I will be billed $29.95 monthly. If canceled within 3 days, I will only pay $2.95 one time. I may cancel my account anytime by calling Customer Care or from My Account.
GET RESULTS NOW
I am coordinator for a Vietnam Veterans group and I have located over
I dated someone for 10 months before learning he had a criminal

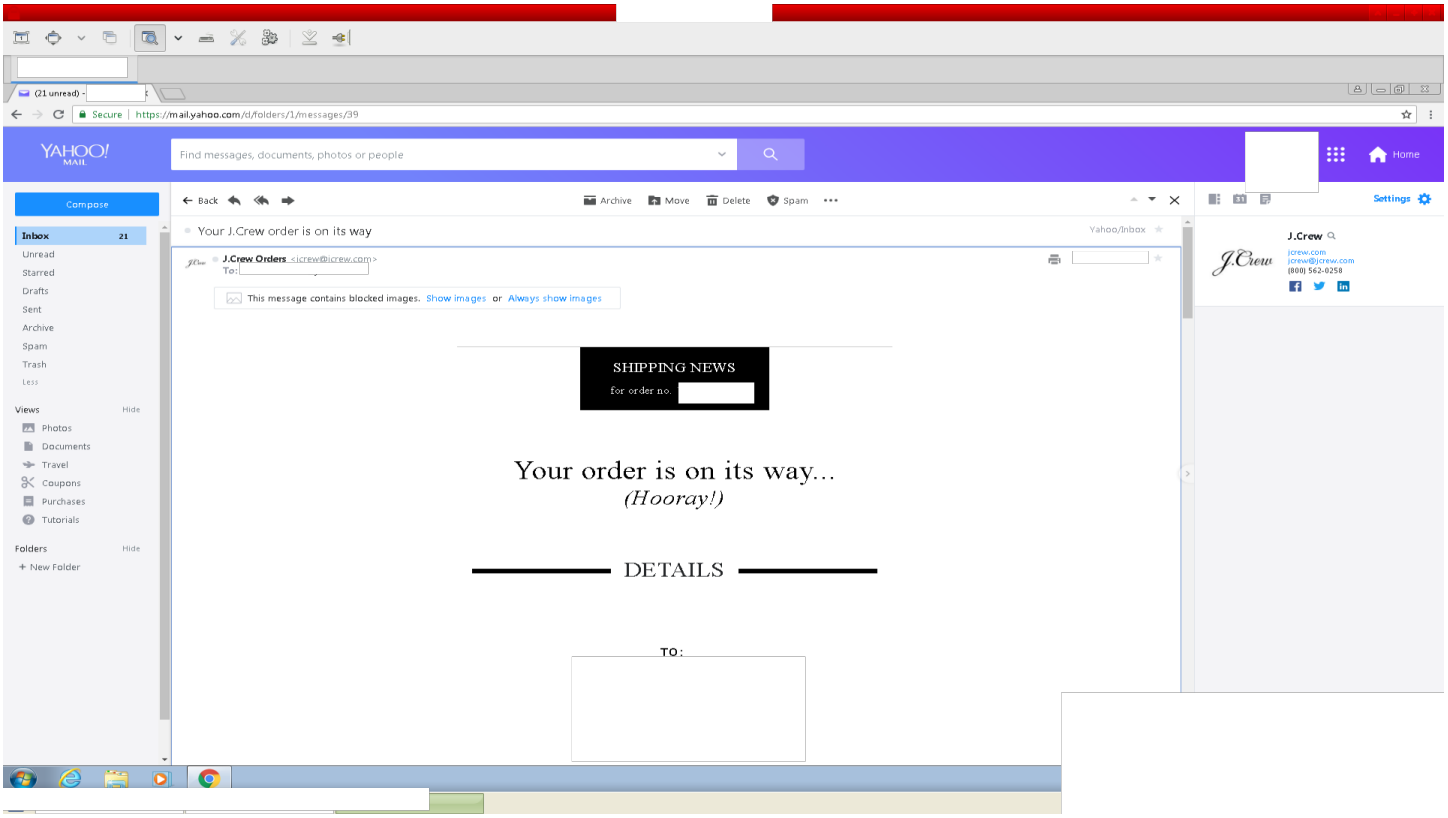

Report
https://www.peoplefinders.com/Reports?sales_order_item_id=61294f20-8ee6-48b3-b4b0-a91c
peoplefinders
Welcome | My Account | Log Out
People Search
Background Check
Criminal Records
Public Records
Reverse Phone
Home > My Account > View Report
California
Age
Birth Month
Birth Day
Birth Year
Update Search
Profile
Property
Addresses
Criminal
Court
Business
Licenses
Comprehensive Background Check
Why is this name different from my search?
Email
Print
Personal Summary
AKAs:
Date of Birth:
6/19/1965
Age:
53
Last Known Address:
Phone Numbers Associated with
No Phone Records Found
Email Addresses Associated with
back to top
No Emails Found
Transferring data from www.gstatic.com...
Report - Mozilla...

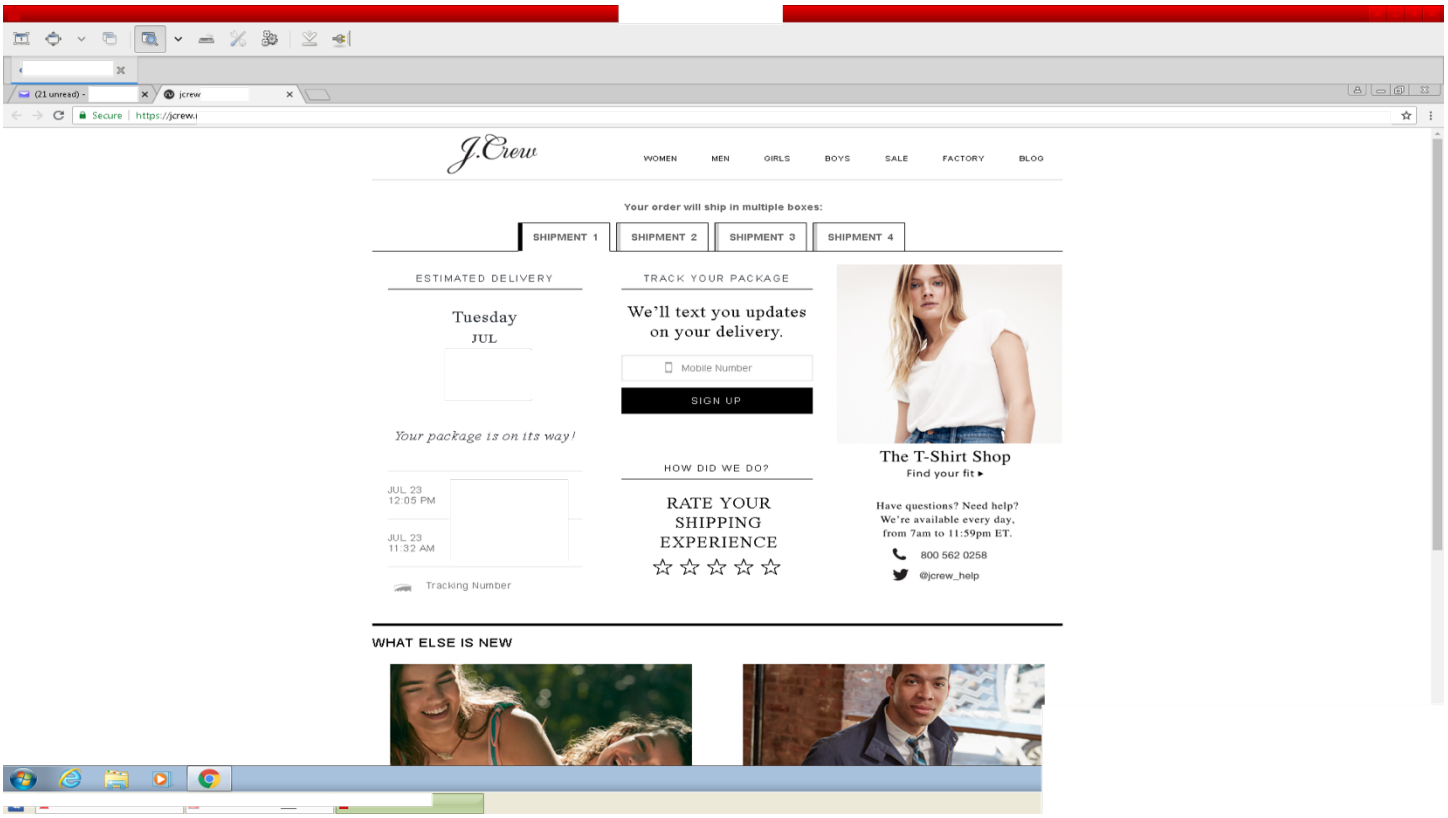
1. Now let's move on to the next successful transaction at the website https://jcrew.com/. First, we will navigate to the website and create an account there with a @yahoo.com email. Once that is done, we will navigate to the account details page and add the victim's CVV details and billing address to the payment page and save it on the account as the default payment method. Remember to do all of this and the steps below in your actual hacked RDP, or it will not work. These websites log your IP address and it will raise your fraud score, leading to a declined transaction if you change it constantly or even once.
2. Next, we will look around the website for something we want to purchase. We need to act like a real shopper to cheat the website into thinking we are a real buyer so we will spend 1-2 hours looking around the website, adding things to our cart, removing them, and then we will leave 1-3 products in our cart, preferably what we want to purchase and let the account rest for 1 day.
3. In the next day, we will make our purchase. Navigate to the website, look around it for around 30 minutes to 1 hour, and then make your purchase, just like the picture below. You should have been successful, and this kind of transaction will not require the billing address to be the same as the shipping as we are not making a purchase of $200+ dollars. NEVER copy and paste the CVV details as the website can easily tell you have done that and will raise your fraud score. Always type everything like a normal buyer would with a CVV on his hand. I do not recommend making your purchases during the night or in the AM time unless it is 8AM or later AT THE CARDHOLDER'S TIMEZONE, the reason for that is because these fraud systems analyze literally everything and people rarely shop during these hours. Also, refrain from shopping during the weekend, do it on the WEEK DAYS ONLY (Mon-Fri). One little slip up could get you declined. You have to always be ten steps ahead of the website fraud systems. And make sure you always choose the fastest shipping method available. For this Jcrew order, I chose overnight, and it arrived the next day at my drop.


Extended today only! 30% off your purchase,* plus extra 40% off sale styles.** Online only. Use code FRIDAY. Details
BACK TO SHOPPING BAG
J.Crew Clothing
CHECKOUT
SHIPPING ADDRESS
SHIPPING & GIFT OPTIONS
BILLING
REVIEW
Please confirm your order
BILLING DETAILS
CHANGE
VISA
$174.96
SHIPPING DETAILS
Overnight – Delivered on or before Tuesday, July 24th
$15.00
GIFT OPTIONS
NO GIFT OPTIONS HAVE BEEN SELECTED
SUMMARY
SUBTOTAL $144.79
Shipping $15.00
Tax $15.17
TOTAL $174.96
PLACE MY ORDER
By placing your order, you agree to our terms of use and privacy policy.
HAVE A PROMO CODE?
Promo Code
APPLY
PROMO: FRIDAY
20% off select full price styles, extra 40% off sale styles
REMOVE
GIFT OR REWARDS CARD?
HAVE A QUESTION?
800 562 0258
LIVE CHAT
what is your return policy?
when can I expect my order?


Extended today only! 30% off your purchase,* plus extra 40% off sale styles.** Online only. Use code FRIDAY. Details
SEARCH
J.Crew
STORES
MY ACCOUNT
BAG
NEW ARRIVALS
WOMEN
MEN
GIRLS
BOYS
SALE
FACTORY
SHOP WOMEN'S SALE
SHOP MEN'S SALE
SHOP GIRLS' SALE
SHOP BOYS' SALE
ORDER COMPLETE
PRINT
THANK YOU FOR SHOPPING AT JCREW.COM
(YOUR CLOSET WILL THANK YOU TOO.)
ORDER NUMBER:
BILLING DETAILS
VISA
$174.96
SHIPPING DETAILS
Overnight – Delivered on or before Tuesday, July 24th
$15.00
SUMMARY
SUBTOTAL $144.79
Shipping $15.00
Tax $15.17
TOTAL $174.96
TOTAL SAVINGS: $64.20
PROMO CODE
PROMO: FRIDAY
20% off select full price styles, extra 40% off sale styles
HAVE A QUESTION?
800 562 0258
LIVE CHAT


Thanks for your J.Crew order
J.Crew Orders
J.CREW
WOMEN MEN GIRLS BOYS SALE
Thank you for shopping at J.Crew
(Your closet will thank you too!)
Hi, MIRO! We've received your order and will get started on it right away. You can expect to receive a shipping confirmation email soon.
Order Number
ORDER DETAILS
Payment Method
$174.96
Shipping Address
Shipping Method
Overnight
Delivered on or before Tuesday, July 24th.


Your J.Crew order is on its way
J.Crew Orders
SHIPPING NEWS
for order no.
Your order is on its way...
(Hooray!)
DETAILS
TO:


J.Crew
WOMEN
MEN
GIRLS
BOYS
SALE
FACTORY
BLOG
Your order will ship in multiple boxes:
SHIPMENT 1
SHIPMENT 2
SHIPMENT 3
SHIPMENT 4
ESTIMATED DELIVERY
Tuesday
JUL
Your package is on its way!
JUL 23
12:05 PM
JUL 23
11:32 AM
Tracking Number
TRACK YOUR PACKAGE
We'll text you updates on your delivery.
Mobile Number
SIGN UP
HOW DID WE DO?
RATE YOUR SHIPPING EXPERIENCE
The T-Shirt Shop
Find your fit ▸
Have questions? Need help?
We're available every day,
from 7am to 11:59pm ET.
800 562 0258
@jcrew_help
WHAT ELSE IS NEW

ACCOUNT-TAKE-OVER FRAUD

Now this is where things start to get really interesting, and where the big money lies in. You ever wanted to card thousands of dollars' worth of electronics and resell them for a quick, big profit? With this method this is completely possible, however that doesn't necessarily mean it is easy. Account-Take-Over is when a fraudster poses as a genuine customer, gains complete control of an account and then makes thousands of dollars in unauthorized transactions, sometimes even maxing out the account and clearing out all the funds available. Lucky for you, I am an expert in ATOing accounts and today I will teach you everything there is to know about this fraud technique.

To even attempt an ATO, you will need to understand a couple of things. First of all, is NEVER use CVV checkers that charge cards. This will burn cards instantly. I personally recommend bit2checker.com if you want to check cards. They don't charge your cards and are fairly easy to use. They charge $0.01 cents for dead cards and $0.02 cents for live cards, which is a great price. Alternatively, you can use try2services.cm which is also a very reliable service. I personally prefer to simply call the bank myself using a burner phone, spoofed with the CVV holder's phone and check the balance, credit access line, recent transactions and more using the automated prompts. To spoof your phone, simply use spoofmyphone.com, they are a great service and allow you to pay them in BTC. Alternatively, you can use the service Many fraudsters used spooftel.com, however they recently blocked toll-free numbers, so we can't use them to call banks anymore.

Any transaction that involves an Account-Take-Over should be considered a LEVEL 3 CARDING transaction. As previously mentioned, these are transactions above $300 dollars and up in value. Usually below $2000 however, as most cards will get flagged for transactions above that number regardless of the ATO. You can always make multiple transactions of $1000-$2000 however with ATOed accounts through the span of a few days to a few weeks and max out the card.

If you call a bank using your burner and the automated prompt tells you the account has been closed for security reasons or the system automatically transfers you to an operator when you type the card number, that means the card is dead and useless, ditch it and move on. Keep in mind that some banks will require the victim's SSN to access the account balance and menu prompt, Chase however does not have this feature so it is considered the easiest for such a purpose although it is the hardest to ATO. I recommend that you note down everything the automated prompt will give you including most importantly, the account balance, credit line access and recent transactions (up to 10 in case they ask you for it). The below picture is an example of what you might want to do.

Once you have called the bank and checked everything, you should have the victim's balance, credit access line and recent transactions. With this information you know how much you can spend on that card. However, there is still one more obstacle we need to tackle, this is the fact that most high security websites such as Newegg, TigerDirect, Neiman Marcus, Stockx, Saks… will refuse to ship to an address that is not in file with the bank. To solve this, we will take over the victim's account (ATO).

To do this, we will call the bank, talk to an operator and first request a change of the primary phone number. Remember, this will require SOCIAL ENGINEERING, which is something that requires training and experience. Don't act nervous, act like you own the account. Remember you are the account owner, why would you be nervous? This is your account. Would you ever call your bank and act nervous? I doubt. To do this, you will need to have the following information from your victim in hand and preferably memorized.

- Full CVV number, expiration and, CSC code.
- Full billing address
- Date of birth (and don't forget to write down his age as well)
- Social Security Number
- Mother's Maiden Name (if you can't find this, first try his middle name, and if that doesn't work then just try guessing using common last names in the background report)
- Background Report
- Closest relatives date of birth (you can get this by carding their background reports)

The most commonly asked tokens are MMN, SSN, DOB, billing address and card details. All the other questions are only available through public records and will not be asked by the first operator you get, only by the FRAUD DEPARTMENT. The Fraud Department is a department that you can be transferred to if you answered any questions wrong from the first operator or if he suspects you are nervous and conducting an ATO on the account, that's why it is very important to keep cool.

If you try changing the phone number and the bank asks for a one-time passcode that will be sent to the cardholder's phone, tell them you no longer have access to the primary phone on file with them since it was disconnected recently when you changed phone carriers. Give them your burner number, receive the text and give it to them, that should work fine. If the system does not allow them to send a text to your burner, then they will transfer you to the fraud department. At this point, I recommend you hang up the phone as soon as they put you on hold, since the fraud department will most likely not be able to conduct the change on the account either and they will end up burning the card by telling you they will give you a call back in 24-48h and they will first try the card holder obviously. Hang up and let's try another way.

At this point you have 2 choices. Either conduct a SIM swap on the victim's phone number by calling his phone carrier and claiming your SIM was damaged/stolen/lost and you need to port it to a new phone you just bought with a new SIM (this will require all the details needed to conduct an ATO as well and if they ask you for the account PIN just tell them you forgot, which will lead them to asking you security questions on the account or trying some other way, which should work fine if you have the required information on your victim). This will also require a NEW BLANK SIM FROM THE CARDHOLDER'S CARRIER.

Your next option is a little tricky and you will require 2 burner phones. First, you will call the bank with the first burner and tell them to send the one-time passcode, however before you tell them to send the passcode you will have to tell them to hold for 5 minutes while you get your cellphone since you don't have it with you at the moment, during that hold call the cardholder with your 2nd burner number SPOOFED to the bank's toll free support number (e.g. 1-800-935-9935) and social engineer him into giving you the one time passcode, you will have to be fast with this. Below is an example of how the dialogue would play out.

- "Hello there, may I speak with Mr. Jason Bourne please?"
- "Speaking"

- “Hi there, this is James Magnolia calling on behalf of J.P. Morgan Chase Bank Fraud Department, we are calling you to conduct an identity verification as we have noticed some unusual activity on your account lately, did you call us to change your primary billing address on file?”
- “What? NO! I didn’t try to change my address, what is happening??”
- “Okay Mr. Bourne, nothing to worry about, I would like to first apologize to you for this inconvenience on behalf of Chase and its partners, but apparently someone has tried to impersonate you and change the primary billing address on your account on file with us. Would you please verify your identity for me by receiving a one-time passcode and telling me what that passcode is?”
- “Yes, go ahead”
- “Okay, thank you for your patience and understanding Mr. Bourne, I will have to put you on a brief hold while I send you the one-time passcode. Please keep in mind Chase will not charge you for the text message, but additional charges may be incurred depending on your phone provider.”
- “Okay”
- At this point, put him on “hold”, and get back to your first burner to talk with the bank operator again. Tell him okay I have the phone now, you can send the text message. He will proceed to send the text message to the victim’s phone. Then, you tell him to wait a little bit while you receive the text on your cellphone and get back to your 2nd burner where the victim is on hold.
- “Hello there Mr. Bourne, thank you for your patience, I have just sent the one time passcode to your phone, please keep in mind the code is only valid for 5 minutes.”
- “Okay, I got it, the passcode is 023847027.”
- “Thank you very much Mr. Bourne, give me one second here while I verify your identity with that code.”
- Get back to the bank operator, give him the code he told you and there you go, you have just changed your phone number on file with the bank. Hang up the call and get back to Mr. Bourne.

- “Alright Mr. Bourne, seems like we have you all verified now. Thank you very much for your cooperation and again, we are very sorry for this inconvenience. Do you have any further questions for me?”
- “No, thank you”
- “Awesome, have a great day Mr. Bourne and thank you for banking with Chase”

This dialogue will obviously not go EXACTLY like this, however, if you have all the victim’s information it should be very easy to social engineer him. You can even change this up, and create your own method.

Once you have changed the phone number, let the account sit for at least 5 days. During that time, create an account with the .edu email as instructed previously on the website that you want to card on your RDP and navigate the website every day for 30 minutes to 1 hour, look at the products, click on them, add them to cart, ALL INSIDE THE RDP. Act like a real shopper. Remember, some websites have really good fraud systems in place and think of literally everything, so you really have to be smart with this to trick them into thinking you are a legit shopper.

Then you call back the bank and change the billing address on file. You can also choose to ADD an additional address to the account, it is really up to you. Again, to change this, have the victim’s most commonly asked tokens in hand (SSN, MMN, DOB, billing address, and your burner phone number since it is now the primary one). Once your identity is verified with the tokens and you are inside the account, tell the operator you have recently moved out of your address and would like to update it. They will most likely ask you for the one-time passcode again, but this time this should be a no-brainer since you have the primary phone number on the account set up to your burner and the text will be sent there. Give them the code and update the address, simple as that.

Now once you have changed the billing address, wait 1 day and make the purchase on the website of your choice. Try to keep it under $2000, or the system may flag it immediately, especially since the cardholder never makes such high value

purchases. Enter all the information correctly, your drop address that is now the billing address on file with the bank, and your billing phone number that is the same with the bank as well. Make both shipping and billing addresses the same, this is CRUCIAL. Triple-check everything for accuracy.

You might be greeted by a Verified by Visa or MasterCard SecureCode prompt, however this should be very easy to bypass if you have the required information on the cardholder.

At this point, your order will go through and either one of two things can happen.

1. The order goes through smoothly without any problem, and becomes "pending". You should've received an order confirmation email as well.
2. The transaction gets declined and the website says you need to call your bank. In this case, call the bank and the automated prompt will act as if the card is burnt (transfer you to an operator automatically) and a fraud agent will answer. Tell them you authorized the transaction, but is not sure why it was declined. If you have ATOed the account correctly, then this should be very easy. He may ask you some questions in relation to the victim's background report, but that should be easy to answer as well if you have all the required information. When the agent tells you are all good to go, submit the order again on the website and this time it should go through. REMEMBER TO CALL AS SOON AS YOU GET THE DECLINED TRANSACTION OTHERWISE THE BANK WILL RING THE CARDHOLDER AT THE OLD NUMBER AND YOUR CARD WILL BE BURNT TO A CRISP!
3. At this point you are all good to go and your order should be in "pending" status. You should've also received an order confirmation email and will soon receive an email that your order has been shipped. SUCCESS!

COMMON REASONS WHY ORDERS GET CANCELLED

Many beginners and sometimes even advanced fraudsters, go through a frustrating period in which their transactions constantly get declined. There are many reasons for that and this section should be very helpful to curb such mistakes. I have made A LOT of mistakes since starting this fraud journey, so I hope you can learn from my mistakes and not make them again.

When you place an order of $1000 or more on a website, you need to understand that A LOT of things take place to verify the authenticity of that transaction. Merchants are not idiots, they do not want to lose money, and that is why the biggest ones, with the biggest yearly revenue, have extremely high security measures in place to curb fraudulent transactions. We need to be aware of such measures to make sure all of our transactions are successful. Below is a list of the most common reasons why orders get cancelled.

1. **Billing phone number does not match the one on file with the bank**. This is very common with rookie fraudsters, as they think the website will not check that. However, THEY DEFINITELY WILL and if it's not your burner phone number, but the cardholder's, you might run the risk of them calling the cardholder and burning your card. Always remember to first change the billing phone number on file with the bank to your burner and use that for website purchases, this is CRUCIAL for LEVEL 3 CARDING transactions. If the website does end up calling your burner billing phone number, they will sometimes ask questions similar to the fraud department on the bank, however these are all PUBLIC RECORD questions, which means they will be available on the victim's background report. If you have previously ATOed the account, this should be quite easy to bypass. In some rare cases, they might make a conference call with you and the bank, and you will be asked the usual verification tokens (SSN, MMN, DOB…..).

2. **Carding one website and then in the same day carding another one**. This is another very common mistake committed by not only rookies, but also by some veterans of the carding game. This is bad because multiple high value transactions in the same day will look suspicious in your account and the bank or merchant might flag that and decline your transaction.

3. **Carding websites in the cardholder's time zone from 7PM to 7AM**. Very common mistake as well, and one that I committed myself when starting out. Nobody purchases stuff during the AM hours and so a transaction at that time looks highly suspicious not only to the bank, but to the website's fraud systems as well. I recommend only purchasing during the hours of 8AM to 3PM in the cardholder's time zone. Anything above that is considered risky and not recommended. Also, you do not want a transaction sitting for very long on the person's account, which makes carding in those hours extremely bad. You never know how often the cardholder checks his bank statement online. I've had cards that died within hours and others that lasted months. Once the package is shipped, you can go ahead and card another store, no need to wait for delivery. Repeat until the card is burnt. Once it is burnt, ditch your mail drop and get a new one. NEVER REUTILIZE DROPS FROM BURNT CARDS AS THE COPS MAY BE ALERTED.

4. **Using an IP address with a high-risk score, or high proxy score to conduct the fraudulent transaction**. This is quite probably the most common mistake of this list. I have lost count of how many people I've seen that committed this mistake. I have previously explained what these terms mean in the FRAUD DICTIONARY in the beginning of this guide, so if you're not familiar with such terms, go back and read again. You need to ALWAYS use THE SAME CLEAN, RESIDENTIAL, LOW PROXY AND RISK SCORE IP ADDRESS TO CONDUCT YOUR TRANSACTIONS! I personally recommend RDPs over Socks5. Most websites can bypass the Socks5 and see your real IP which 100% will lead to a declined transaction. This is not possible with RDPs.

5. **Using Linux or Mac OS X to conduct fraudulent transactions**. This is not as common as other mistakes, however I have witnessed a lot of times as well with my customers. The only operating system that should be used to conduct these transactions is Windows 7, 8, 8.1 or 10 RDP. The reason for this is because you want to appear to the website to be a legit shopper, with a LEGIT COMMONLY USED OS, and not some fraudster using Kali Linux/Qubes or OS X, this will make your order get declined instantly. RDPs are also great because they won't leave any trace of the fraudulent activity on your actual HOST OS, which will leave any attempt to recover such logs useless. You can use them, and once you're done with them, never use the computer again.
6. **Using Opera, Internet Explorer, Tor, Brave or any other non-common browser to conduct fraudulent transactions**. I have seen a lot of people commit this mistake, and it is quite common. As previously mentioned, you want to appear to be as generic as possible to the website. You do not want them to flag you as a unique user and a potential fraudster. Using such browsers will cause transactions to be declined and are just not reliable for such purposes. Tor and Brave are just completely out of the question and if you used such browsers to conduct fraudulent transactions, frankly I feel sorry for you. If you want to be successful in this, either use Chrome (best option) or Firefox with 0 ADDONS AND 0 MODIFICATIONS.
7. **Using a CVV with a balance not high enough to successfully conduct the transaction you want**. This is something I see a lot of beginners do as well. They usually get a CLASSIC Visa, and expect to be able to easily card over $1000 in merchandise with that card. This is just not realistic. For that kind of transaction, you want ON THE VERY LEAST a Platinum card. Websites will also flag high valued transactions with such low limit cards instantly, which will lead to declines and headache**.**
8. **Using a shipping address that differs from the CVV's billing address**. This has been explained extensively, and you should already know that ANY transactions that are considered LEVEL 3 CARDING, will not go through without the proper Account-Take-Over and change of billing address to your drop.

You should always keep in mind that NO METHOD IS PERFECT, and the website can cancel your order simply because they do not feel it is safe to process it. Nothing is perfect, but you ATOed the account correctly, it should be very easy. Remember to always stay under $2000 per order and ALWAYS choose the fastest shipping method available. Some say this raises flags, but if you did everything else correctly, this should be the least of your concerns.

MAIL DROPS

Now I am going to get into the topic of mail drops. This is going to be an extensive chapter and I will list many methods to properly acquire drops. Mail drops are one of the most important aspects of your carding setup, because how will you acquire your carded items if you do not have a safe location to send them to and where you can later collect them?

This has to be a place that has absolutely no link to your real-life identity and of which there could be no possible way to be traced back to you or anyone else related to you. Finding a drop is really simple, and the easiest way to find one is to just drive around your neighborhood or walk around if you don't have a car, looking for new, empty houses for sale where you can ship the goods to. I honestly recommend you do this in another city at least 10-15 miles away from your home, as that will place some distance between where you live and your drop. However, if you do not have a car this could be a real problem, so I recommend you just walk around the neighborhood if you have this problem and find a house a couple of blocks away from yours. You can go to zillow.com, craigslist or any other similar website to find houses around your neighborhood for sale, a lot of them will also have a sign up so it's really a no-brainer to find one. You should preferably aim for a house in which the driver cannot see that the house is empty inside, as that could lead the package to be returned to sender. Just use your brain and find a decent house that you think is worth giving it a shot. I have shipped things to houses that clearly looked empty before with no problem, however I do not personally recommend this.

Another thing you have to keep in mind is that those houses are usually owned by someone or a real estate company, and they regularly showcase the house to potential buyers. Try to monitor the house for one day, just park your car outside of it and keep watching, to keep track of who goes in and out of that house and at what times. You don't want owners or real estate agents seeing a note left on the door such as "NOT HOME LEAVE PACKAGES BY THE DOOR" as that could lead to problems (they could contact the police, thinking someone broke in and is living in the house) and an obvious burnt drop and lost package. Use a tape to glue your note to the door and do not use actual glue, as that may lead to leaving sticky paper residue on the door and you don't want the owner to even wonder why is that. You want to be as stealthy as possible so as to not burn the drop, only when the actual card burns. I have had my fair share of mistakes, so learn from them.

You should track the package every day and depending if the package requires a signature or not you will have to apply different techniques. The first method is to just act like you are away and leave a note glued to your front door saying something along the lines of "CURRENTLY AT WORK, PLEASE LEAVE PACKAGES BY THE FRONT DOOR. TRACKING NRS:, FULL NAME, SIGNATURE. You can also optionally print the confirmation page and glue that to the note as well just to make sure. The driver is the one that makes the final decision to leave your package or not, but usually this is not a problem for UPS when they don't require a signature. Leave the note on the door and wait somewhere near the house (this could be inside your car) for the UPS guy. Once you see him leave the packages, wait for him to leave and go over there and pick them up and put them in your car. Next leave the area, open the packages, inspect for any tracking devices and throw away the packaging somewhere that is not close to your house.

The second method is when a signature is required. This will mean you will have to meet face-to-face with the driver and sign the package. Remember TO NEVER ACT NERVOUS OR THEY MIGHT ASK FOR ID. The driver's job is not to investigate fraud, but only to make sure the packages are delivered to the right person. When packages don't get delivered and a claim is filed with the carrier, it is taken out of the driver's own salary, so KEEP THAT IN MIND! You must make him believe the

package is yours. For this, I recommend you have in your hands a print-out of the order confirmation page and the tracking number open on your smartphone (OBVIOUSLY USE A VPN, NORDVPN PREFERABLY), and look like you have been waiting for him. You could do this simply by waiting at the drop, sitting on the front lawn or something similar. Do not wait in your car and then when he arrives suddenly come out of the car. That is very very suspicious and will lead him to ask you for ID.

I also recommend calling the bank's automated prompt system and checking if the card is dead prior to showing up at the address. You do not want cops to outsmart you. When you have the packages, drive to somewhere away from the drop, open the packages, inspect them for any tracking devices, get rid of the packaging and shipping label (burn it if you can) and drive home.
If the card is still valid and there was no tracking device on the packaging, you can keep carding to that drop until the card burns. Get as much out of it as you possibly can before moving on to another one. Once that is done, NEVER SHOW YOUR FACE TO THE DROP AGAIN! Below I will list some more methods to acquire mail drops, you can choose the one you feel most comfortable with.

1. **GENERAL DELIVERY**: In the United States, you can send a package to a USPS office via "General Delivery". Unfortunately to use this drop method you will require a Fake ID as they require one to go pick up the package. There is also the downside of cameras. Example of the format to send package to General Delivery:

JASON BOURNE
GENERAL DELIVERY
160 J ST (POST OFFICE'S ADDRESS)
COSTA MESA, CA 94536 (POST OFFICE ADDRESS)

In addition, a lot of websites do not ship to general delivery, so this is not the best method, however definitely usable.

2. **HOTEL DELIVERY**: This works in pretty much anywhere in the world and it is a very simple method. Pick a big hotel, and send your package there. When it arrives, just go over there with a fake ID and tell them you have a package that arrived for you. Rarely will they require you to give them your room number or anything of the sort to verify that you're staying with them. However, as mentioned, a fake ID will be required most of the time.
3. **WRONG ADDRESS DELIVERY**: This is one of my favorite methods and I have used this many times. Simply pick an address where someone clearly lives in, preferably far away from your house. When your package arrives, just go to that house and tell them you live right down the street and unfortunately you had the package delivered to the wrong address because you confused the numbers. You can also optionally go there beforehand and tell the person living in the house that you put the wrong number in the address and the package was shipped already, which means it is going to be delivered to their house, and also give them your cellphone so that they may call you when the package arrives, or just tell them you will come by when the package is listed as delivered in the tracking. The downside to this is can only use each address once. Use it more and it will obviously look extremely suspicious. No fake ID is needed for this method.
4. **RENT A HOUSE**: This is also a great method. You can rent a house/apartment for one month, massively card items there and once you're done, just leave, stop paying rent and leave no trace. You can also card that house rent if you prefer. This can be done through Airbnb. Or just pay cash up front. You can find a bunch of people on craigslist that will accept cash. Unfortunately for this method, you might require a fake ID.
5. **EMPTY HOUSES/HOUSES FOR SALE**: This one is very easy and it was described above in detail.
6. **RENT A MAILBOX**: This is one of my favorite methods as well. A lot of places will offer private mailbox rental (UPS offers this service at a lot of their stores). They will receive and sign for any packages, and you can go in and pick them up (they offer you the option to open the mailbox even when the store is closed, so I recommend you only go when nobody is there and the store is closed). Massively card items to the box until your card is burnt and

then never show your face to that store again. Pay in cash or with a Vanilla Visa or other prepaid untraceable card. Unfortunately, most if not all services will require some form of picture ID for this, so a fake ID will be a requirement. I recommend you do not use a picture that can be traced back to you, use a picture that looks like you or just blurry the picture with photoshop and make some slight modifications so that it is not possible to identify you. If the cashier asks anything about the picture, improvise, say it is old or that there was a problem with the DMV/GOVERNMENT picture. This is because they will most likely scan the ID and keep a record of it.

7. **SETUP A MAILBOX**: Find a trailer park where everyone sets their own mailboxes on the road. Simply add a box to the end with a non-existent lot number shortly before you expect the package. NEVER do this in your own trailer park or home town.
8. **SETUP A RESHIPPING COMPANY**: This is a much more advanced method. You will need to open accounts in any popular job site that is available and used in your area, an example of this in the United States would be craigslist. Then from there, you would make an ad as a reshipping company that is looking to employ new people and get them to work as soon as possible. Make a good sales pitch. To make the ad more attractive, I highly recommend you create a logo for the company (you can get logos for $5 on Fiverr) and a detailed description just to explain what the company is about. You need to look as legit as possible. Leave in the description a form that the job seeker will have to fill out to get this job. ADDRESS, FIRST AND LAST NAME, AGE, NATIONALITY, NIN (National Insurance Number for UK, or SSN for USA, each country has its own system). You will also have to ask the job seeker to send a CV (so you will have his picture and more details about him).

Make sure to also tell them in the description that “NO PREVIOUS EXPERIENCE IS REQUIRED”, so that everybody knows they are qualified for the job, and you will have more people and more addresses to use. Those details should be sent to the email you put on the ad. Tell them in the description that a response will be sent as soon as the application is received. Once you get all their details, message them with your email and tell them that they are accepted for the job, they will only

now have to send a recto/verso of their ID, with their sort number etc… in short, all the details you need to make a cash deposit in their account. “Payment will be made at the end of each week by cash deposit” is what you should tell them. Now, you can choose to simply not pay them and only use them for a week, or pay them with cash deposit as mentioned. The best option would be to just pay them to avoid any kind of trouble or complaint, they could go to the police and that would be a problem.

So, the email response you will send them should look something like this:

“Thank you very much for the job application, you have been approved. Please provide us with a recto/verso of your state ID and your bank account number. Payment will be made by cash deposit at the end of each week.”
There are many reasons why we ask for these verifications. One of them is to simply be able to pay the person. The other is to steal and use their identity in case they decide to steal your packages or do anything that you don’t like, essentially blackmail. To let them know “your identity is fully known and you could be in trouble if you try to steal a package”.

So, once the person sends you the details, you will tell them about how the job works. This, that, those items are coming this day of the week, you are expected to receive them, and a call will be made that day to know if you indeed received it.

You will have to call the person to confirm that they have received your packages, otherwise you might go to their house for nothing, you do not want this to happen. You will have to purchase what is called a “Parcel Drop Box” to receive the mail, as you do not want any form of contact with the person you hired. You do not want them to know who you are or even your face for that matter. You can find such boxes at home depot website, and sometimes at their actual store (https://www.homedepot.com/p/ParcelWirx-Graphite-Wall-Ground-Mount-Secure-Locker-550200200F7081/302976323). I highly recommend you print a big logo of your “company” and stick it on the side of that parcel drop box. This will raise no suspicion and the people you hired will be very happy to be making a

quick buck to do basically close to nothing. You will come a day or two before you plan to card, and drop that box in front of their porch and leave. Message them a couple minutes later and let them know that the “Parcel Drop Box” or “COMPANY NAME BOX” has arrived, and tell them to leave the packages in the box. For bigger packages, you can give them the combination to the parcel drop box.

From there, you can card a bunch of stuff, track it, and when it arrives, simply come by the person’s house and pick your stuff up. You don’t even have to look at them or speak to them face-to-face, which is the actual goal of all of this. If you decide to pay the person and keep working with him, just leave the box there and keep coming for the products once they are delivered. If not, just pick up the box and leave. Be the one to have their numbers and use a burner to call them, also spoof your number if you can. Calling with a burner goes without saying.
The same process will be applied to each person you hire. When you describe the job to them through your email, you will have to choose and tell them how much you want to give per package and signed letter. I recommend $10-15 for each normal parcel/package and $20-25 for each signed one. This should be a great pay for doing almost nothing, and I doubt anyone would refuse.

I also highly recommend you go pick up the packages using a Windbreaker jacket with the company’s logo printed on it so that you can wear just before picking up the packages. Nobody would ever question or wonder what you are doing this way. Fraud is an art and the smoother things go and the more average joe you look, the better it is. Have all your “application forms” ready beforehand so you could just email it quick and easy to each person. Always conduct business well and smoothly, you could use one of those persons for other jobs in the future, such as a bank drop or something of the sort. In the UK this technique is very easy, there are a lot of eastern Europe immigrants and Asians. A lot of students will pick up on those offers and most likely live in flat shares. They could care less about what is happening, they will be satisfied to get that little extra easy cash. Same goes for other countries, in USA you could use anybody that responds, or some illegal Mexican, or whatever you prefer. The possibilities are endless and there are always so many people looking for work and extra cash. REMEMBER: TELL YOUR

WORKERS TO NOTIFY YOU BY EMAIL IN ANY CASES OR PROBLEMS WITH A PACKAGE AS SOON AS POSSIBLE.

To summarize, you list ads on the max number of job sites you can find that are quite known in your area, also use direct sites such as craigslist, gumtree etc. Explain what the company is about but not too much in details, just something like: We are XYZ Company. We specialize in XYZ and we need workers as soon as possible, no experience is required. Please send a CV to our email at yourcompany@gmail.com, and you shall receive a response shortly. Make everything look as legit as possible, use a nice clean logo and make sure there are no typos/spelling mistakes in any of the forms. You need to look professional. When you get a response with their CV, reply and tell them congratulations, blah blah blah… you are accepted, please complete the attached form (send them a form where they should fill all their info, NIA or SSN, Scan of ID recto/verso, and two proofs of residency. As previously mentioned, the required details will vary depending on the country you live in, however you will need the bank details to make the required cash deposit. After you receive the form and all the other stuff, explain to them the job, tell them the task will be to receive packages and sign for them if so needed. Card, call/or send them an email a day or two before, telling them what will the item be and the name on the package. Call them the day the package gets there, get confirmation and collect. ALWAYS LOOK THE PART AND MAKE IT SOUND/LOOK/FEEL LEGIT!!

The danger in this is very small, but minimizing it is the goal. If there is an issue, the person never really saw or spoke to you. If anything occurs, you are just a worker recruited online and wearing your job jacket. It will be for the best to have a back-story setup. As have the “company” employment emails in your mailbox going back and forth. Have a whole story setup that can be used as your alibi if anything goes wrong. The more security the better. The parcel box will always be next to their porch and easily accessible, let them know that and it should be obvious as well.

Another thing to keep in mind is before going to the area to do pick-ups, look the street in Google Maps, this way you will know from which street/corner to come and from where to leave, where you could park your car or take transports. The good thing here is that if you feel there is something dodgy going on, all you have to do is keep walking/driving without stopping. But something dodgy is very unlikely to happen with this setup.

CHARGEBACKS

One questions I see a lot of beginner fraudsters asking is, when the card is declared stolen and the transactions are disputed because of fraud, who will lose money? The answer is, it depends. In the case of a PHYSICAL CARDING transaction using chip & ATM PIN in countries where such technologies are used, the bank will take the hit and lose money when the transaction is declared fraudulent.

In all other cases, such as online fraudulent transactions, where the person disputes a charge by calling the bank, the merchant will take all the loss. Let's say you card Amazon for $2000, they will pay about $1600 for the merchandise that they sent you, and they are short the money because you carded them, so they will have to make 6 similar big orders without problems to cover that loss. This makes it easy to understand why they are so strict and worrying when it comes to fraudulent transactions, and why most big retailer websites have a lot of securities in place to curb such transactions. Big merchants like Amazon, Newegg, and TigerDirect will simply take the loss and assume that they failed in detecting the fraudulent transaction, but smaller merchants can potentially make a formal complaint at their local police department.

The questions is, will the police investigate? It depends. If a merchant reports a $200 loss, which is unlikely, for an order shipped out of state using a stolen credit card, there is a 99% chance that the police will not even open an investigation into that. In contrast, if they report a $5000 loss using a stolen credit card from the same state and shipped in a nearby city, LE might move for that. It will also largely depend on the number of complaints, the amount of loss compared to the size of

the city, and whether there is an obvious pattern between fraud complaints or not. You should try to make your orders un-linkable to each other, and use your common sense to avoid creating a pattern that could lead to an investigation. It will also depend if the cardholder himself decides to make a complaint or not. As long as the bank refunds them (which in 95% of the cases they do), then they will most likely not care and just move on with their lives, cancel the card and get a new one.
With that said, there are definitely some people who might feel very angry and want to make a police report for identity theft. Again, there will be an investigation if there is an obvious pattern in your fraudulent activity. It all depends which city we are talking about here. REMEMBER: when you card a website, they take the loss in case of a chargeback, so they are going to do everything they possibly can to protect themselves. You have to be smart and ask yourself, if I were in the shoes of the website owner(s), how would I catch fraudsters? What securities would I have in place? This will vary immensely depending on the pricing of the merchandise available throughout the website and the size of that website, how long it has been online, and different factors.

WARRANTY FRAUD

Warranty fraud is a complex form of fraud, and it works amazingly for any company that offers warranties for its products. This occurs when a fraudster exploits warranty policies for their own benefit. Early last year, fitness tracker creator Fitbit found itself at the center of a complicated warranty fraud scheme. When the company's customer service department noted an unusually high volume of warranty claims, it began investigating the source of these claims. The company found that detailed customer data had been posted online and subsequently used by hackers to take control over customer accounts. Using these stolen accounts, the perpetrators were able to file false warranty claims to take advantage of the company's defective product replacement policy.

I have used this exploit extensively throughout the years with a great success rate. I have gotten some $1000 CPUs from Intel and motherboards from ASUS using this trick. Here's how it works. A lot of companies, especially electronics, offer what is called "advanced RMA". This is a type of warranty replacement policy where the company will send you the new product first, along with a return box for you to send them the defective item. This is where we can take advantage of this system.

This will work with Dell, Intel, NVIDIA and ASUS, and most likely a lot of other companies, however these are the ones I personally have experience with so far. One technique you can use to file such fraudulent warranty claims is go to eBay and ask sellers for serial numbers of their products, which most will give you without any questions. Or you can simply card a product and request an RMA using its serial number. Call the manufacturer, say that your product is defective and you would like a replacement (tell them you tested it in some way and you are sure that the specific part is the one that is defective, e.g. "the video card shows nothing on the monitor, I tried with other 2 perfectly working monitors and still nothing, however when I tried changing the video card it worked fine"). Then ask them if they offer advanced RMA, and the answer will most likely be yes. If they ask you to pay for shipping, use a LEVEL 2 CARD and ship to your drop.

When you receive the package, take it, and don't contact the company again. For Intel, they will ask for the 5 lines of text on the CPU itself, and a credit card for putting on file, so you need to have the unit in your hands for this to work. For ASUS, the serial number is enough, however they will require a credit card. For DELL, which is the easiest, no credit card is needed, just order the item and the only thing you need is a name and a drop.

I highly recommend you try this with different companies and find the ones that I haven't discovered yet. There are literally dozens of companies out there that offer advanced RMA, and there is a lot of money to be made, all you need is motivation. I have seen a lot of people use this method to get a free Xbox One from Microsoft. Most companies require that this warranty claim be done over the phone but do not worry, it is simple and most of their employees don't seem to care about their job or whether or not you are stealing from them.

HOW TO PICK THE BEST CARDS

If you don't have access to FULLZ, or you have a CVV shop/seller that you want to get the most out of it, there is a trick that will save you money, but it will require some patience on your part. This will work with any CVV shop as long as you can see the name and ZIP code of the CVV holder.

First, you are going to search for any BINs that you want. This will vary depending on what you want to do exactly (426684 & 438854 work well for ATOs). If you can't search by BINs, just pick CREDIT CARDS from any bank. Once you are in the list, find cardholders that match your gender, and for each one, do the same thing. Search their name and ZIP on ssndob.cm and check if you can find them. A lot of the times you won't, especially if the cardholder is under 45 years old, so just do the same thing until you're able to successfully find one. When you have the DOB and SSN of the cardholder, before buying the card, do this to check if you can get his info online.

Go on peoplefinders.com and get their background report (card it). Check if the DOBs match, and if the address list matches too to make sure you have their SSN and DOB 100% accurate. When you are sure, buy the card and buy the SSN & DOB. You now have the victim's FULLZ. You can go to archives.com or ancestry.com to get their Mother's Maiden Name (MMN). To do this, simply card an account on any of those 2 websites, get their mother's name on the background report, and search using her first and last name, and correct date of birth. Search for "marriage" records, and if you can't find any, just search for "birth" records. If you can't find anything still, just try searching for the victim's father's marriage records. Please note that not every state has their records made public, so it is possible you won't find this at all. This is completely fine, just try guessing using the cardholder's middle name or by trying common last names in the account when you're ATOing. By doing this, you can select only the best cards from your autoshop. If you're buying cards from me, I do this every single time before sending you cards from my databases. If you also need FULLZ, I can get that for you for an extra fee, so feel free to contact me if you need help.

COMMERCIAL FRAUD

This is yet another and most likely easier method to card products. This method works best for Canada, but works great in the USA as well. First, you need to find any major provider that only sells products to commercial customers. For computer parts for example, you can target ASI, Synnex, and so on. The goal here is to get the business registration certificate of a business in the town where your drop is located. This certificate is usually public data and can be found on the registration records depending on which state or province you are located in. Once you have that from a business that operates in the same field of activity you wish to get the products for, you are ready to hit the provider.

Apply for an account on one of these providers using that document, put all the business information in the form, but put a drop address close to the business instead and your burner phone number. Both providers (ASI and Synnex) usually don't call, but just in case, better to put your burner. It usually takes 24-48h for your application to be reviewed and approved. "Your Name" is the name of the real business owner. On the credit application, do not request net terms, just write "no credit" and let them know you will pay before getting the products shipped. On the credit card authorization form, put the cardholder's name, address, card number, expiration date, CSC code and all the rest. Let them know that this person is an "officer" at your business, such as a remote sales representative. Once the application is approved, you are good to go and hit big amounts. The reason for this is because they do not make verifications when sending orders, as they rarely get fraudulent orders. They assume that commercial customers are always going to be legit, but in fact, we use someone else's business documents to trick them into thinking you are the business owner. I was able to pull over $5,000 per order using this technique as the merchant is considered low-risk so there are very few declines, and verifications are almost non-existent. With computer parts, it's extremely easy to do that, and you can try many commercial providers. Now you are playing in the big guys' game, and the possibilities to this are endless. Make sure you never show your face at the drop once the card burns, as they will really go after you and try to find what happened.

NEWEGG & TIGERDIRECT

You ever wanted to card these 2 big merchants to get some electronics? In this section I will explain to you how to do this. This is normal difficulty if you know what you are doing and have some experience with social engineering. You will need the following information for this.

- Cardholder's account ATO and billing phone number & shipping address changed to your burner and drop, or address added on file with the bank
- Full background report on the cardholder
- Story about why you're shipping to that address
- Familiarity with the cardholder's area (restaurants, shopping malls, and similar points of interest)

NEVER use mail forwarding companies to ship your products. Those companies are blacklisted by such merchants and will lead to an instant decline. Which American would use a US card to ship to a forwarding company to get the product out of the country? None. Have a normal drop address. Familiarity with the cardholder's address might seem kind of odd, but some people, including myself, have been asked questions such as "can you name a local restaurant near your house" to make sure you are really the cardholder, so it is definitely not a bad idea to get familiar with the surroundings (major points of interest) in case that happens. You'll thank me later.

Register on the website using a .edu email in the name of the CVV holder. Take your time to browse, look around, click on products, read descriptions, put them in cart, act like a real shopper. Once you have done that for 4-5 days, the account is ready to card. Send the order and try not to go over $2000. The order will be placed on "hold" and you will have to talk to the verification department. I will describe how this works with TigerDirect, but Newegg is pretty much the same.

The will ask you for your addresses, credit card information, then you will have to pass VBV/MCSC prompt. Next, they will ask for your date of birth. Then, 3 verification questions will be asked. These are all public record information and are available through background reports, so if you have done everything else correctly this should be a no-brainer. Try to have as much information about the cardholder as you possibly can find. Try to have so much information that you feel like you personally know the cardholder. Answer the 3 questions and be quick about it. If you fail one, you will be asked an additional question. If you fail 2 or more, forget the order. Once you send everything, your order will be on hold and you will need to call the verification department. Below is an example of how the conversation might play out.

- "Thank you for calling TigerDirect verification department, would you provide me with your order number please?"
- "123456"
- "Okay, what is your name?"
- "Jason Bourne"
- "Thank you Mr. Bourne, let me verify your order for you." (he will place you on a hold for 1-2 mins)
- "Thank you for holding Mr. Bourne. Is <NAME ON THE PACKAGE> a tenant at the shipping address?"
- "Yes" (answering this wrong will void the order"
- "I wasn't able to locate that person in the system. So, you will be offered 2 options. Either we ship to your billing address, or you need to call your bank to add that shipping address as an alternate address on file so we can process your order"
- "I already added the address with my bank"
- "Oh really? Okay, then let me verify that for you. Please wait." (you will be on hold while they call your bank, sometimes they will even make a conference call with your bank)
- "Okay, I see the shipping address is on file. Thank you, and is it okay if I call you on your billing phone number 123-456-7890?"
- "Yes, sure"

- “Thank you, just one second” (the phone will ring, pick up the call or your order will be voided)
- “Okay, seems like we got you all verified Mr. Bourne, thank you very much for your patience. We will have your order shipped out to you tonight”

Pay attention to the pitfalls in the dialog above. You must assume that the shipping name is a tenant at the address if you’re not using the CVV holder’s name. For example, if the cardholder’s name is Jason Bourne, you can ship to a Michael Bourne and tell them it is your son, but make sure that name is on the background report and you have their DOB. Sometimes they may ask you for it in case they get suspicious. Next MAKE SURE YOU PICK UP THE PHONE WHEN THEY CALL THE BILLING NUMBER. If you did everything correctly, your order should go through smoothly. They do not ask for document scans, everything will be done over the phone.

WALMART

Walmart is one of the biggest online retailers, and it is absolutely incredible to card. If you know what you are doing, carding this website is very easy. You can choose to apply a LEVEL 2 CARDING OR LEVEL 3 CARDING technique to this website, it is up to you depending on the value of what you want to card. However, I highly recommend you use Walmart for LEVEL 3 CARDING operations since it is such a great website that we can take advantage of so easily. They usually don't do any type of manual verification for orders below $700, anything above that will require the same process we used for Newegg & TigerDirect.

First, I recommend you get a MasterCard platinum or above. Below are some of the BINs that work great with Walmart, with such cards your order will be shipped even if the card is burned after the order is placed.

- 424631
- 438857
- 426428
- 540168
- 482860
- 485620
- 426685
- 426684
- 400022
- 430023
- 551149

Next, register an account with Walmart using a .edu email in the name of your CVV holder (OBVIOUSLY DO THIS INSIDE THE CLEAN PROXY/RISK SCORE HACKED RDP AS CLOSE TO THE CARDHOLDER AS POSSIBLE), example if his name is Jason Bourne make the email jbourne93@my.college.edu (I have a tutorial for getting a free

.edu email in this guide if you didn't read it). This looks authentic and will CONSIDERABLY lower your fraud score.

Then click on "My Account" and add your CVV (don't copy and paste it), address and phone number. Then just navigate the website for 30 minutes to 1 hour and close your browser (don't sign out). Let the account sit for 2 days and login during these 2 days, navigate the website just like you did before, click on products, read descriptions, ACT LIKE A REAL SHOPPER. Once that is done, you have 2 options for your transaction.

As mentioned above, you can choose to make this a LEVEL 2 OR 3 TRANSACTION, it is up to you. If you want to do a transaction of more than $700, keep in mind it will go under manual verification and they might ask for more details, such as giving you a call, similar stuff to Newegg and TigerDirect which honestly should be very easy to bypass if you did everything correctly. If you want to go the other route and make a transaction below $700 in value, then it should go through smoothly automatically and you should receive a shipping confirmation email soon if you did everything correctly. REMEMBER TO CHOOSE THE FASTEST SHIPPING METHOD FOR HIGHER SUCCESS RATES!

Enjoy your newly carded product and easy money!

AMAZON

No guide about fraud would be complete without touching on Amazon. It is literally the biggest online retailer at the moment, and Jeff Bezos' net worth clearly confirms this. They are very easy to card and they don't seem to care much about losses and security, probably because of the amount of legit transactions and money they get on a daily basis worldwide.

First we need to go to Amazon and create a new account using a .edu email in the CVV holder's name inside our clean proxy/risk score RDP. Once that is done we need to navigate to the email and activate our account by confirming the email. After that, we will need to navigate the website for a good 30 minutes to 1 hour again, close your RDP, and as previously let the account sit for 2 days. Act like a real buyer and navigate the website every day during these 2 days, search for products, look at descriptions, read reviews, stay 3-5 min on each product page (this will trick the website into thinking you are reading all of that extra bullshit, which means you are a legit shopper interested in the products), also add some of the products to your cart, could even be the products you plan on buying.

At the end of these 2 days, we are ready to card. Go to Amazon, login and clear out everything in your cart if you left anything there. Navigate the website for 30 minutes and add the products you want to card to your cart (I recommend staying 3-5 min on each of these products' pages to make sure the website analyzes you as a legit buyer that cares about his money, especially for large purchases). REMEMBER TO STAY BELOW $2000 AND ALWAYS CHOOSE THE FASTEST SHIPPING METHOD AVAILABLE. To speed up the order, start a chat window with an Amazon support operator, and tell him some kind of excuse as to why you need the product fast (e.g. you purchased a $800 camera and told the operator "I urgently need this camera or I will fail my class/work deadline").

They might ask to call you on your BILLING NUMBER for orders above $800, but if you did the ATO correctly, that should not be a problem at all. If no ATO was conducted on the account, try to limit your purchases to $500 max.

Once your order is approved you can go higher as your account will be trusted regardless of the ATO. But always stay below $2000. Max out the card as quick as you possibly can before the owner notices. The securities in place on Amazon are really just bots and formulas they use to analyze you as a real buyer and not a fraudster. If you fail you may get limited or blocked so pay attention.

This method works 90% of the time. Also keep in mind these websites are upping their securities every single day, so this may not work anymore in a few months. TAKE ADVANTAGE OF THIS WHILE YOU STILL CAN!

AMAZON GIFT CARD METHOD

Carding Amazon gift cards is not relatively easy, as it requires some experience with social engineer and it is time consuming. With that said I will present you guys with 2 methods that I have personally used in the past and that currently still work. The first one works great, but it is time consuming and it doesn't involve carding really, just social engineering. The second one is an actual carding method.

Find a seller on eBay, craigslist or some other platform of your choice that is selling $25+ Amazon gift cards. You will message them asking to see three and only three consecutive numbers so you can email Amazon and make sure the card is legit, and not some fake stuff. You might find some sellers reluctant to do this, but from my own personal experience, most will comply no questions asked.

Once the seller has sent you pictures of the card, take note of the 3 consecutive numbers. You will then pull up a live chat on Amazon, while you are already logged into the platform using a throwaway account and tell them something along the lines of "My uncle Greg told me he has gotten a $<VALUE> Amazon gift card for his 60th birthday, but unfortunately the card was damaged in the back and so the numbers are unreadable, so he gave it to me as he said there is no use for it. Is there any possible way that you guys can help me with this and solve this problem?" OBVIOUSLY MAKE UP YOUR OWN STORY, DON'T USE THIS ONE OVER AND OVER AGAIN AS THEY WILL QUICKLY CATCH ON.

Next, the Amazon support will inform you that they can add the card balance to your account, all they need is the 3 numbers, which you have it. Go ahead and give it to them. The representative will then proceed to add the balance to your account, enjoy the money!

If you find a stubborn representative, just close the chat and find a new one. I recommend you don't go over $150 with this method.

Now, for the second method, which involves carding.

You will first get a US CVV (Visa works best). Once you have the card, create a .edu email registered under the name of the cardholder, then go to Amazon.com and select gift card. Pick a design and amount. Put the name you are sending to with the same last name as the CVV. Then simply click add to order and create a new account with the .edu email, fill in all the details and make the order. Simple as that. Obviously follow all the details outlined in this guide and you should be 100% good to go. At this point, after reading so many tutorials on each website, you should have a pretty good idea of how everything works, and know that carding ANY website is just a matter of skill.

AMAZON REFUNDS

This is a very simple technique to getting a refund or a reship on basically any Amazon product. I have used this more times than I can possibly count and always got 2 of everything, especially shoes. This method is very noob friendly, and can even be done on your legit account, with your legit card, just don't abuse it if you plan on going that route or you will have problems coming your way.

You will buy anything off Amazon, then when the product arrives, you will just pull up an Amazon support chat and tell them in some way that the product was damaged or missing (e.g. "I ordered an Adidas shoe, but when I opened the box I was extremely disappointed to see that I only got 1 shoe, is there any way we can fix this with a reship or can I possibly get a refund?"). Another example could be "Hey, I have just received my package. The package itself was in perfect condition, there were no scratches, marks, dents or any kind of physical damage to the package. The package was still sealed and nobody else opened it. However, once I opened the package I saw that the item inside was broken, can I please get a refund for this or a reship?".

With that done, they will proceed to send you the reship or refund, whichever you prefer. Refunds, the balance can be added to your Amazon account if you prefer instead of being returned to your bank account, which means you can do this with carded products. However, do not do more than 5 refunds in one month from the same account, or they will quickly catch on and block you. And make sure you have other legit orders mixed with no refunds before doing this.

GET FREE FOOD FROM KFC/MCDONALDS/BURGER KING AND OTHER FAST FOODS

This method is very simple and does not require any carding at all. Ideally you don't want to be eating this crap, but in any case, I will lay out here a method that will give you free food for any of these places in case one day you do want to go there and eat with your family/friends for free.

Simply create a new Gmail/Yahoo/Hotmail account with a legit looking name (e.g. richardabbott95@gmail.com). Then, go to the website of the fast food that you want to eat at. Select customer support or try to find an area to submit a complaint. Once you have done that, write a detailed email explaining something such as "Hello, I want to file a complaint against the mentioned store. I have gone to the store at 123 FAKE STREET, CITY STATE 20384 during my lunch break at 1:00PM Monday MM/DD and I went through the drive-thru, and ordered 6 big macs for me and my co-workers. I got my order and drove away, however once I got back to my workplace, I realized I was only given 2 BIG MACS! EVEN THOUGH I PAID FOR 6! I am extremely disappointed with McDonald's and be sure I will not be coming back, this is ridiculous, how can a staff be so incompetent?"

They will proceed to give an answer within 24-48h or give you a call in the number you provided. Once they do, they will give you a voucher for a free meal at one of their restaurants. I've had different results with this, with this particular 6 big macs method, I was able to get 8 free big macs.

I also did something similar with KFC (said I got a bucket big only 4 pieces were inside), and they sent me a $25 voucher on the mail.

Again, ideally you do not want to be eating this crap, but for you guys that are struggling to make ends meet, by all means, do whatever is necessary.

BURNER/DISPOSABLE PHONES

This is most likely one of the most important aspects of your fraud setup. You will require a burner phone in the same country of your CVV holder to conduct an ATO on the account. 99% of the websites will also require some form of phone number that they can call to confirm the order, or just in case there are any problems. Without it, you will not be successful in this and your orders will most likely not be accepted. It is very important that we stay within a cheap budget as well to not spend too much money, we want to MAKE money not LOSE money. However, too cheap cellphones may prove themselves unreliable for such purposes and may actually lead to failures (I have seen this before). In this section I will go in-depth into this topic and give you guys my own setup for this.

First I highly recommend you create an account with RingCentral.com. This website is used to create a burner phone number that will ring your burner cellphone whenever someone calls you. The will ask for a phone number where they can reach you when registering. You can make an excuse and tell them you are at work and will call them ASAP. Call them and tell them you will be traveling for a few months and you need an IP phone to call home for free. They will offer you an office plan, accept it.

Once you have your RingCentral account set up, take some time to explore the interface and learn how to use it, how to register phone numbers. You can select by state and city to register phone numbers and point them to your burner cellphone. They often change their interface so I rather not go into much details here, however make sure all the burner numbers you created on the website will ring your burner cellphone.

To get a burner cellphone, this will vary a lot depending on the country that you are located in. In the United States, Canada and most countries you can easily buy a prepaid SIM card at any retailer for $30-$40 with no ID and false information (not someone else's identity). Some countries will require ID, so you will have to work around that, find someone that will sell you such SIM cards for cheap no ID.

Using a burner cellphone without RingCentral is definitely a possibility, however I do not recommend this, since one, these calls can get traced, and two, your cellphone IMEI will get flagged eventually and banks will know you are a fraudster calling, which will make your attempts to defraud useless. You can also choose to always call banks using a spoofing service if you prefer, which will give you the same results, although probably more expensive then RingCentral. AND MAKE SURE TO KEEP YOUR PHONE ON ALL THE TIME WHEN EXPECTING A CALL AS SOME MERCHANTS MAY CALL YOU TO CONFIRM AND IF YOU DON'T PICK UP YOUR ORDER WILL GET CANCELED. Keep in mind also that LE can subpoena spoofing services to see your real cellphone, so do not use your REAL cellphone under any circumstances, unless you want to go to jail, in that case go ahead.

Use RingCentral + Spoofing Service for maximum security.

CARDING FLIGHT TICKETS

One thing I see a lot is customers asking me how do they card flight tickets and if there is any danger to it. I also see a lot of vendors selling such services for a fee. I recommend against using such vendors and against carding such things, as that can usually be dangerous. However, if you still want to do it, I will explain here how to conduct such a fraudulent transaction the safest way possible so as to prevent any mishaps.

If you are carding a local flight, there is usually no danger involved. You should use a card from the same country as the country you are currently flying in. You will put your real name, or put the cardholder's name and use a fake ID. If you choose to use your own name, make sure you have evidence to support your case if you get pulled over while boarding or getting out of the flight. Say you purchased the tickets from craigslist or some kind of forum, but have the evidence to support this. You want to avoid any and all suspicions in case things go south. Better to be safe than sorry. If you use your real name, DO NOT USE YOUR PASSPORT TO BOARD THE FLIGHT, USE ANOTHER TYPE OF NON-GOVERNMENT IDENTIFICATION! This could be something like a fake student ID, and in many cases they will accept this. Present a government ID only if asked to do so, but never a passport.

Carding international flights, now that is a whole other ballgame, and much harder. You will have to use your real name and passport number, which poses a serious risk. Be aware that they can't prove you carded the tickets yourself, so a chargeback will not make you a suspect as long as you took the necessary precautions on your computer when purchasing the ticket. Show the ticket on check-in and go to self-check-in to avoid people as much as possible. Try to card a short flight and ALWAYS AVOID FIRST CLASS AS THEY RAISE FLAGS. Upon arrival, get out of the airport as fast as you can.

Never card the airline directly, always use a third-party website such as Expedia, Cheapair, etc.. as they can't move fast enough to catch a carder. If you card them successfully, the chances of getting caught are slim.

Now when it comes to carding hotels, I do not recommend under any circumstances. You do not want hotel security or police knocking on your door at 3AM to talk about a chargeback or fraudulent transaction. If you go on a trip, feel free to card a part of it, but it is common sense that you have money if you're traveling. Don't have money, don't travel, that simple.

Card only one-way flights and do not card return flights unless they are very close to each other (2-3 days max). If there is a chargeback and you are waiting for your return flight, be sure that they will wait for you and arrest you. Last but not least, have really strong arguments beforehand to use if you get intercepted at any point, always be prepared for the worst. Leave absolutely 0 proofs of carding.

COMMON REASONS WHY YOUR CARDS GET BLOCKED

Having a card burn after you have just purchased and gone through an extensive process to acquire information on your target and ATO their account, can be a frustrating experience, as well as getting declined transactions. In this chapter, I will be brief, but I will explain some of the most common reasons why cards get blocked. From this you can pay attention to certain things and not commit these mistakes.

Credit card companies are continually upping their anti-fraud security measures to curb such activities, constantly upgrading their security software and techniques. The thing is, sometimes even legit buyers get flagged because of these securities. Why is that? Well, there are many reasons and this is mostly because something looks bad to a credit card company and they would rather have you confirm your identity before authorizing the release of your money in their possession, then trusting merchants' security systems and losing money. Each card company (Visa, MasterCard, American Express, Discover…) has their own security technologies that look for anomalies in your spending habits. Each transaction is analyzed for up to 200 different data points, everything from where you live to what you normally buy to how much you're spending, to determine the likelihood that you're the one actually making a particular charge. If the analysis doesn't add up, your card will be blocked and your next purchase declined.

But what exactly triggers a block? Card issuers don't go on record about specific red flags for security reasons (they don't want us fraudsters knowing their secrets). But according to experts and hapless cardholders who have experienced a block, these shopping habits below may lead to hassles.

- **SHOPPING FROM A LOCATION WHERE YOU NEVER SHOPPED BEFORE**. A buyer quoted “I’ve had calls from my card company saying, we’ve detected some unusual activity. It wasn’t unusual, but it was a different pharmacy than the one I normally go to”. This is why it is extremely important to get an RDP as close as possible to the CVV holder’s address or previous RECENT addresses as possible. And obviously, the RDP needs to be non-blacklisted, with clean risk and proxy scores.
- **MAKING SEVERAL PURCHASES QUICKLY**. One example is a buyer that sometimes hits three grocery stores in a row to find what she needs and take advantage of sales. But a few months ago, was so speedy that by the time she swiped her card at the third store, it was declined. She quoted “I called the bank when I got home, and they told me that shopping at three supermarkets within an hour or so was considered ‘unusual activity’.
- **CHARGING SOMETHING SMALL, THEN SOMETHING BIG**. This is very commons as fraudsters like to sort of test the waters with a stolen card by first charging a tiny amount, say a song on iTunes or even using a charged CVV checker (never use such checkers), before moving on to a big purchase. That small to big pattern in the CVV holder’s buying patterns can potentially lead to a declined/blocked card.
- **SHOPPING AWAY FROM YOUR HOME**. This is very common when someone moves from one place to another. A fraud expert quoted “If my billing address is Massachusetts and I’m buying a washer and dryer in Idaho, that is an anomaly, because why would I buy a washer and dryer in Idaho if I live in Massachusetts?”. Another reason why RDPs are so important.
- **CHARGING TRAVEL EXPENSES**. On the road, any purchase from gas to restaurant meals can trigger a block. While that’s long been true for travelers abroad, it now happens domestically too. A buyer quoted “Once my travel to L.A. was flagged and I spent 20 minutes verifying transactions”. When she asked what caused the card to be declined, she was told “a taxi, a charge at the airport, in-air Wi-Fi and a rental car hold” – all standard travel expenses.
- **YOU HAVE REACHED THE CVV’S CREDIT LIMIT**. This is pretty much self-explanatory and I shouldn’t have to go into details.

- **BUYING THINGS IN DIFFERENT GEOGRAPHIC LOCATIONS ON THE SAME DAY**. During a cruise, one buyer, used a card to get money from an ATM on the ship, then she later made a purchase on-shore in Belize. For the rest of the trip, her card was declined". Apparently, the ATM on board the ship is registered to a Miami location, and several hours later, she was purchasing something in Belize. To the bank, it looked very suspicious because the transactions happened so close together. Online purchases to merchants in different parts of the world can trigger the same flag.
- **DEALING WITH BILLING ISSUES**. A buyer wanted to make an addition to an online purchase, he contacted the company, but the second transaction they tried to process was declined. The card issuer "thought that the merchant was taking advantage of her card number".

HOW TO HANDLE A BLOCK

When your card company suspects fraudulent activity, sometimes you will get an email or a phone call asking you to verify a purchase. Other times your card is simply declined, with no advance warning and no information why, and it's up to you to call the issuer and sort out the problem. If you have previously conducted an ATO on the account, this should be very easy. Just call them, answer public record questions about the CVV holder, and your card is authorized.

One thing you can also try if you're not ATOing the account, is to simply call the bank having the CVV holder's information in hand and tell them that you're traveling and just want them to authorize any charges, say you had problems with this in the past.

BEST LOW-SECURITY CARDABLE WEBSITES 2018

CLOTHING

- https://www.jcrew.com/
- https://www.levi.com/
- https://www.gap.com/
- https://www.nike.com/
- http://us.asos.com/?crd=true
- https://www.buckmason.com/
- http://us.boohoo.com/
- http://www2.hm.com
- https://www.uniqlo.com/us/en/home/
- https://www.forever21.com/us/shop
- https://www.amazon.com/
- https://www.landsend.com/
- https://www.electriqueboutique.com/
- https://www.tmlewin.co.uk/
- https://us.oki-ni.com/
- https://www.denimio.com/
- https://store.wizkhalifa.com/
- https://ghostly.com/
- http://www.kitbag.com/
- https://g-eazystore.com/
- https://www.danielwellington.com/us/
- https://www.imenapparel.com/
- https://www.theiconic.com.au/
- https://gnrmerch.com/
-

ELECTRONICS

- https://www.walmart.com/
- https://www.amazon.com/
- https://www.overstock.com/
- https://www.vova.com
- https://www.frys.com/
- http://www.electronicexpress.com/
- https://www.mouser.com/
- https://www.shopclues.com/electronics-offers-zone.html
- https://www.jameco.com
- https://www.outletpc.com/
- https://www.abt.com/
- https://www.buyradardetectors.com/
- http://tcc-qatar.com/
- http://www.rugift.com/
- http://www.radarbusters.com/
- https://www.lmc.com.au/
- https://griffintechnology.com/
- http://mag.divineo.cn/magento/
- http://shop.panasonic.com/
- http://www.world-import.com/
- https://www.tmart.com/
- https://www.controllerchaos.com/
-

OTHER

- http://www.windpowersports.com/
- https://shop.ronjo.com/
- https://www.hayneedle.com/
- https://www.yesasia.com/us/en/home.html

- https://www.alittleluxury.com.au/
- https://www.goldenmine.com/
- http://www.uhrbox.de/
- http://www.cloncom.com/
- http://addr.com/
- http://www.innovations.com.au/
- https://samples4.com/
- http://www.send2fax.com/
- https://www.bullguard.com/
- https://www.whiskygalore.co.nz/
- https://champagnegallery.com.au/
- https://www.transparent.com/personal/
- https://www.trionworlds.com/en/
- https://ghostly.com/
- https://www.lorenhope.com/
- https://www.doordash.com/
- https://www.pizzahut.com/
- https://www.etsy.com/
- https://www.fandango.com/
- https://www.sunfrog.com/

Please keep in mind I have compiled this list, assuming one has taken all the necessary steps in order to successfully card explained in this guide. Some of the websites have different security features, and so you may or may not face some problems. If you do, it should be really easy to go around such issues. Usually all it requires is some form of confirmation, easily obtainable. Some websites may ask for ID scan, in that case you can go to the resources below this section and navigate to secondeyesolution.

This list was compiled in July 25th 2018. Some websites may have been shut down or may have upped their security since then. Good luck on your carding and enjoy!

CARDING RESOURCES

RDP PROVIDERS (FROM BEST TO WORST)

- xDedic (xdedicvhnguh5s6k.onion) - HACKED RDPs
- Me! I can get you RDPs from xDedic if you don't have an account there, alternatively I also offer invites to the website for purchase.
- UAS (http://uas-service.ru/login/) - HACKED RDPs
- FlyDed (http://www.flyded.com/) - HACKED RDPs
- AMinServe (https://aminserve.com/) - NON-HACKED RDPs

ADDRESS VALIDITY CHECKER

- https://www.ups.com/address_validator/search?loc=es_US
- https://smartystreets.com/
- https://www.edq.com/free-address-lookup-tool/

CARDING FORUMS

- omerta.mn
- crdclub.ws (mirrors club2crd.cc, crdclub.su, crdclub4wraumez4.onion)
- verified2ebdpvms.onion
- crimes.ws
- enclave.ac
- korovka.cc
- ru.wt1.pw
- cardmafia.pw

CVV

- Me! I offer 90-95% valid, freshly sniffed CVVs from my very own hacked databases for very cheap. Message me for more details.
- https://yalelodge.ru/
- https://epicmarket.pw
- gocvvx6uywahobt6.onion
- http://st0n3d.su/
- http://uniccshop.ru
- C2bit.pw

BACKGROUND REPORTS & TELEPHONE/PEOPLE/BUSINESS SEARCH

- https://www.instantcheckmate.com/
- https://www.beenverified.com/
- https://radaris.com/
- https://www.intelius.com/
- https://whitepages.plus/
- https://www.411.com/
- https://411.info/
- http://www.addresses.com/
- http://www.abcheck.com/
- https://www.anywho.com/whitepages
- https://infotracer.com/
- https://www.emailfinder.com/
- https://www.freephonetracer.com/fcpt.aspx?_act=Homepage
- http://infospace.com/
- http://www.lookup.com/
- https://www.ussearch.com/
- https://www.mylife.com/
- https://www.peekyou.com/

- http://www.peoplebyname.com/
- https://www.peoplefinder.com/
- https://www.peoplefinders.com/
- https://peoplelookup.com/
- https://www.peoplesearchnow.com/
- https://www.peoplesmart.com/
- https://www.phonedetective.com/
- https://pipl.com/
- https://www.publicrecords360.com/
- http://www.reversegenie.com/
- http://www.reversephonelookup.com/
- https://www.salespider.com/
- https://www.searchbug.com/
- https://www.spokeo.com/
- https://www.superpages.com/
- https://thatsthem.com/
- http://www.usidentify.com/
- http://www.yasni.com/
- https://www.yellowpages.com/
- http://www.zabasearch.com/

FULLZ SELLERS

- Me! I can get you US/UK Fullz, message me for more details and pricing!
- @Goldmarket (DREAM)

BIN CHECKERS

- http://bins.pro/
- https://bincheck.org/
- https://www.bincodes.com/bin-checker/

CVV VALIDITY CHECKER

- http://bit2check.com/
- https://try2services.pm/
- http://ug-market.com/

SOCKS5

- https://luxsocks.ru/?dc=1
- https://www.911proxy.re/

SELLERS WORTH CHECKING OUT

- @6LACK (WSM)
- @DEUSXMACINA (WSM)

VPN PROVIDERS

- https://nordvpn.com/
- https://www.blackvpn.com/
- https://cryptostorm.is/

COMMUNITIES WORTH CHECKING OUT

- https://www.reddit.com/r/privacy/
- https://www.reddit.com/r/privacytoolsIO/
- https://www.reddit.com/r/security/
- https://www.reddit.com/r/netsec/
- https://www.reddit.com/r/TOR/
- https://www.reddit.com/r/SocialEngineering/
- https://www.infosecurity-magazine.com/

CONCLUSION

Well, we've reached yet the end of another guide my friends. I first want to thank you and congratulate you for making it this far. You are a dedicated individual and deserve a pat in the back for all the knowledge you have sunk in your brain. I hope this tutorial opened the eyes of a lot of you guys. Even I was able to learn a couple of things extra. That has always been my method to learn more, teaching others.

I would like to kindly ask you to leave me an honest, detailed feedback on one of my Dread posts below, you have no idea how much that helps me. Building reputation and having great feedback is one of the most important things in creating a great business, you will be greatly contributing to my success, which I will definitely appreciate!

dreadditevelidot.onion/post/8021a9fa7d4fdc54e4cb
dreadditevelidot.onion/post/3e463bccc64f72d80fd2

Below are links to all current guides that I have available at the moment. I will have many more great stuff on the way so be prepared for that!

ULTIMATE BANK DROP SETUP & EXPLANATION GUIDE 35+ PAGES:
dreadditevelidot.onion/post/5b0f6e6770b51bbb7bf7

COMPLETE FRAUD EXPERT SETUP TUTORIAL 100+ PAGES:
dreadditevelidot.onion/post/f93bbee2154b3e13dec0

Here are some more links you will find useful!

MY DREAD PROFILE: dreadditevelidot.onion/u/Bailopan

MY WALL STREET MARKET PROFILE/SOON TO BE VENDOR PAGE:
wallst4qihu6lvsa.onion/profile/Bailopan

MY DREAM MARKET PROFILE/SOON TO BE VENDOR PAGE:
t3e6ly3uoif4zcw2.onion/contactMember?member=Bailopan

To end this guide, I would like to thank you again for reading, and ask you to please feel free to contact me if you have any questions. I will be happy to help you out, that's what I am here for! Below are my contact details!

TOX: bailopan@toxme.io
JABBER: bailopan@exploit.im