CARDING

YOUR OWN MASTERMIND

- By Cyber Mate & Cracking Factory

I have included most if not all of my knowledge from this part of the business in this Class. For many of you who have read my previous classes, 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 class 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 class, 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.

We are not only teaching u carding but we will also teach how payments are processed to reduce the chances of u getting failed.

This tutorial will not be same as other niggas books who just made a 1 post tutorial and proves them self as carders

Just stay with us and concentrate on every point.

What are 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 CODES:

Many fraudsters think tha 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 and 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^1103101000000001000000000300000

0?;

- % 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

- 0000000010000000003000000 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.

So guys this much is totally enough for now next class will. Be at evening, till then read each and everything again and again, and if something is not clear do not hesitate to google that.

Guys this is really worth reading. This is not same as taught on telegram this is the real carding.

Bit difficult but highly safe with very very (0.001%) less chance of getting caught

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.

Some of u might think wtf is this?

So this is real carding shit and not that 10 lines method which says blah blah!, this is what carding tutorial is

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 (yes i am sure u guys never heard that) , 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.

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 or u can say paise dene ka time" 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.

Some of u will still think what is this so this is important to know u will know got to know Nd one more thing do take it seriously and read again and again

This is really worth reading

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

I m telling this type of stuff so that u can understand how payment process done after applying cc cuz if u kow how is that happening than there will be ofc less chance of failure and if u know how payment process in transactions nd which steps are followed than u can use proper safety to all of them in order to get good anonymity with less failure chances.

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

traditionl 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 yeah lol that's damn freaky but tho if u read it again and again with the help of google u will grab gold tho idec if u read it thoroughly or not

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, 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 is the card holder, I think that's obvious and so not explaining much.

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 even India don't use avs for smooth transactions cuz

we do know most of the Indian users are less educated and don't even know how to use card, if there will be an address verification system than some people will. Not be able to do that lol and so Indian cards are non avs (usually debit ones)

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 which is basically known as otp.

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 Secure Code 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 Secure Code 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 i think this much discussion is enough on 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, India don't use ssn

numbers instead india use aadhar card number which is more safe than ssn

Why?

Cuz ssn is 9 digit number and aadhar card is 12 digit number and even Indian government distributed aadhar card to nearly 111 crore Indians nd so Indian security is ok. But still. India falls on 9th position globally on most attacked country lol

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.

U can think. Of ssn as aadhar card of Americans niggas

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 as like india. Example, let us say your mother's name was Mary and she was born into the pandit family. Her maiden name would be "Mary pandit".

Then, let us say, she married your father, whose name was Tom rajput. When she married him, she became Mary rajput.

That is her married name, but her maiden name will always be Mary pundit.

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/

This much is enough for bin i guess

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)

If u think above is trash than consider me worthless, cuz i prefer security rather than carding.

Cuz if u have a good cc than carding is as simple as using ur own cc with some extra precautions so what matter here is security, perfection and company's trust (that's most important cuz if any service think ur order as suspicious they can get u hell)

This much is enough for proxy score let's move further

One more thing some carders say without proxy u can do successful carding so here is what i think

Why u wear pants while going outside? U can go naked but still u wear pants why? Cuz for personal. Privacy and to save ur self from disrespect and so that's what proxy do

Consider it ur pants lol

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.(yes u heard right? People usually blame cc for being unsuccessful but sometimes problem is in core)

Anything above 1.00% will lead to declined transactions most of the time.

MAC ADDRESS:

I know all of u r familiar with this but many of u face difficulty bout this 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 class I will explain how to mitigate this risk.

VIRTUAL PRIVATE NETWORK (VPN):

I know everyone knows this but still for the safe of completion ek baar bata diya.

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

MAC

A MAC address also known as a media access control address is a unique 48 bit number identifier assigned to network interfaces.

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:

Again i know most of u know bout this but ma toh bataunga muje ap pe vishwas ni ha.

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 that 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.

So guys' yaha pe common terms wala topic khtm hota ha carding me

Operation security

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 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.

For the fuck sake u guys don't want to spend 10 years of imprisonment for 500$ (35k rupees right?)

And some people think that there are many carders on tg doing for cheap so the truth is they r kids and there for money only. First of all most of them are fraud and if some of them r legit than they don't know they r inviting cops to their doorstep in near future

Always remember, if you want to be a criminal, then do your homework, or don't be a criminal.

Think like cops and search for ur weak points

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.

Super-duper highly recommended from Mine side.

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.

As I have mentioned previously in the fraud dictionary section of 1st class, 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 site,

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

Always remember one mine golden point:

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.

#1

We need to use an extra clean hacked residential Windows 7 RDP . 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

. (yes use them as it is, no script addons makes u fall. Under category of suspicion i kmow many nigga carders think add ons are necessary bit let me tell u my friend, a website can easily detect addons and which

makes u look suspicious, i don't know if u r getting mine point or not but that's true)

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 naughty American city, we want a CVV from naughty american city.

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 lol,.

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 th

If the .edu email method doesn't seem to be working for you, then you can simply card a domain with ipage.com which is blocked now but find more like this 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.

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 lol).

I know. Many of u are thinking this is too much but hey man this is necessary for more than 500$ items,

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 we have already discussed that above

List of private and secure search engines:

Search Encrypt

https://www.searchencrypt.com

It is a search engine with a focus on privacy.

DuckDuckGo

https://duckduckgo.com

The search engine that doesn't track you.

Startpage

https://www.startpage.com

The most private search engine in the world.

Qwant

https://www.qwant.com

The search engine that respects your privacy.

How to change the GPS coordinates in the Chrome / Chromium browser (but this is not physical GPS) with HTML5 Geolocation, despite the city with VPN / proxy / SSH / its IP.

1. Open the Chrome / Chromium browser, go to the site (for the test) https://www.w3schools.com/html/html5_geolocation.asp and click the Try It button (in the notification the browser asks to allow geo, we allow)

2. Press F12 (the page for developers opens).

3. Open the secret handshake function for developers by pressing the key combination (for Windows, Linux) Ctrl + Shift + P (for MacOS) Cmd + Shift + P.

4. Find "show sensors".

5. In the lower part of Geolocation, select the desired city (you can add a city by indicating the GPS coordinates.)

6. On the site, click the Try It button again, the location has changed.

USA NON VBV BIN LIST

==========

BIN: 400022

Country: US

Vendor: VISA

Type: DEBIT

Level: CLASSIC

Bank: NAVY F.C.U.

==========

BIN: 430023

Card Brand: VISA

Issuing Organizaion: WORLDS FOREMOST BANK

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: CLASSIC

Issuing Country: UNITED STATES

==========

BIN: 438949

Card Brand: VISA

Issuing Organizaion: COMMERCE BANCSHARES, INC.

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: PLATINUM

Issuing Country: UNITED STATES

==========

BIN: 488893

Card Brand: VISA

Issuing Organizaion: FIA CARD SERVICES, N.A.

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: PLATINUM

Issuing Country: UNITED STATES

==========

BIN: 426429

Card Brand: VISA

Issuing Organizaion: BANK OF AMERICA, N.A.

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: PLATINUM

Issuing Country: UNITED STATES

==========

480012

Card Brand: VISA

Issuing Organizaion: FIA CARD SERVICES, N.A.

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: GOLD PREMIUM

Issuing Country: UNITED STATES

==========

BIN: 486236

Card Brand: VISA

Issuing Organizaion: CAPITAL ONE BANK (USA), N.A.

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: PLATINUM

Issuing Country: UNITED STATES

==========
======

BIN: 441297

Card Brand: VISA

Issuing Organizaion: FIRST NATIONAL BANK OF OMAHA

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: PLATINUM

Issuing Country: UNITED STATES

==========
=====-=

BIN: 401398

Card Brand: VISA

Issuing Organizaion: U.S. BANK NATIONAL ASSOCIATION ND

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: PLATINUM

Issuing Country: UNITED STATES

==========
=====-=

BIN: 426428

Card Brand: VISA

Issuing Organizaion: FIA CARD SERVICES, N.A.

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: PLATINUM

Issuing Country: UNITED STATES

==========

BIN: 416621

Card Brand: VISA

Issuing Organizaion: WORLD FINANCIAL NETWORK NATIONAL BANK

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: CLASSIC

Issuing Country: UNITED STATES

==========

BIN: 431307

Card Brand: VISA

Issuing Organizaion: FIA CARD SERVICES, N.A.

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: SIGNATURE

Issuing Country: UNITED STATES

==========

BIN: 441297

Card Brand: VISA

Issuing Organizaion: FIRST NATIONAL BANK OF OMAHA

Card Type (DEBIT/CREDIT/CHARGE): CREDIT

Card SubType: PLATINUM

Issuing Country: UNITED STATES.

==========

Brothers, woke up !? There is a common misconception among ordinary people that the balance is on a credit card, but this is not so - the money does not physically lie on it, the credit card is like a pass to the card account in the bank that issued it. In other words, it carries out the identification of the account holder - whether he can take money from that chest that is in the bank.

Bank card parsing

The merchant passes the card through the POS terminal - a device that reads the information recorded on the magnetic stripe of the card and contacts the bank to conduct a transaction, which connects to the processing center and transfers the data from your

card there. Further, the processing is associated with the issuing bank that issued the card and receives a confirmation or refusal in the form of a code. The successful authentication code is 00 -

APPROVED (approved). Otherwise, they get a ban on the deal, often beaten in Hollywood films ("sorry, your account is frozen" and the demonstrative cutting of the card with scissors). A payment system like VISA connects all the links of this chain together, for which it charges up to 3.5% from each transaction.

What is a dump?

A dump is a collection of information recorded on the magnetic stripe of a credit card. Consists of three tracks (tracks). The first two are used directly for the operation of the card, and the third track is intended for recording various service information. The most important is the second track. The first track duplicates the basic data of the second - card number, expiration date, CVV - code, and also contains the name of the card holder.

Where can I get dumps?

There are currently three ways. Portable readers are being manufactured or purchased - tools for reading the magnetic stripe of a payment card. The smallest readers that I have come across were the size of a matchbox and were made in Ukraine by Boa Factory engineers. Further, the devices are handed out to cashiers in boutiques and expensive stores, waiters in restaurants, currency prostitutes, and they pass a client card not only through a legal POS terminal, but also through their reader. A large processing center of a bank or trade network is hacked, through which payments of physical (not virtual) stores, hotels, restaurants pass, and the base of their customers is obtained. They are simply bought from those who took possession of them in one of the above ways.

Write a dump to the credit card itself

This requires a special device called an encoder. They are sold completely legally and cost $ 800–1000. The most widespread model in carders' circles is MSR 206. I connected it to a computer via a USB port, inserted a dump into a simple program, passed the card through the slot - and you have in your hands a magnetic copy of a card of some American "Buratino".

Is it already possible to go to the store with such a card?

No, it's too early to go to the store, since we have a duplicate of a real card, but it's on a piece of white "plastic" (usually CR-80). The seller in the store will be very surprised if you offer him such a card.

To avoid this, you need to negotiate with the seller in some decent store, such as: "Vasya, I have such garbage, I'll come to you, take a laptop and plasma, then we'll sell and the loot in half." It works - the owners of restaurants, boutiques and casinos gave us 40-50% in cash of the amount that they "rolled", and we told them that they need to answer their bank if problems arise.

And here are the problems. Sooner or later, the real cardholder (card holder) will appeal the payment. He complains to his bank, those to VISA, and now strong guys from the bank's security service, who installed a POS terminal in this casino, rushed to our casino. They will come and say: "Well, you rascal," roll "fake cards?" Well, here our oligarch should open his eyes wider and say: "I don't know anything. Now I'll call the cashier who worked that evening. " Calling Masha.

Bankers to her:

- Did you check the validity period of the card?

- Sure.

- Was the cardholder's signature on the back?

- And then. I even compared her with the signature in his passport. And he signed on the slip in the same way.

A slip is a check that comes out after paying for the goods by credit card. All information about the purchase is printed on it: time, date, organization name, details of the place where the purchase was made. By the way, the data for the slip is taken from the first track. And if the dump does not care what name you indicate in the first track - the real owner of the card or the name indicated in your "left" passport, then the card number must still be written in the original, otherwise the payment (transaction) will not work.

And that would, of course, not be bad: you stupidly acquire a "left" passport, you stupidly go with it to any bank in any country and just as stupidly open an account with a debit card. As a result, you have a credit card with the name of Zhenya Sokolov with $ 5 on it and a passport in the same name with your photo. You erase all the data from the magnetic stripe on figs, take a dump from those that you have, change the name in the first track to Zhenya Sokolova, write this dump to the card and go - even to the bank, even to the store.

You ran out of money on this dump - you erase it, prepare and write a new one. And so, until Zhenya Sokolova starts looking around the globe for all banks and all shops. Then you buy a new passport and go around again. Well, if they begin to recognize in person - then only plastic surgery then.

The bankers will ask if the cashier checked the card number and surname on the check and the front surface of the card - the cashier will answer that, of course, yes, he will add that the card was not damaged and there were no signs of forgery, and this "interrogation" is over - with all suspicions the bank has no legal basis to block the payment. Of course, if sellers in Minsk stores checked whether the data on the slip coincided with the numbers on the card itself, it would be impossible to turn an already used card into a reusable one, but in Belarus, a country of frightened idiots, cashiers everywhere “scored” the rules for safe service bank cards and I often managed to make purchases from dumps recorded on original, but expired, or even on discount cards.

Businessmen who owed money to crime bosses and who had no choice were often involved in working with white "plastic". Of course, we did not “milk” one point too often, otherwise the servicing bank could select the terminal and we would be left without work at all.

Do you know what a PIN is?

Each of you will answer that these are four digits, without which you cannot get cash at an ATM. Right. But I will add.

First, a PIN code is often required when paying for purchases. And secondly, the PIN does not have to be four digits. Its length should be large enough to minimize the likelihood of its selection by trial and error, and on the other hand, small enough so that the cardholder can remember it. Therefore, the length of the PIN varies from four to twelve digits. More often, of course, four.

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

Basic knowledge of clothing carding

Introduction:

CC - credit card information

Fulka - great credit card information

Cardholder is the legal owner of the card

Shop - online store

Spike - the process of buying goods in an online store using stolen credit card information

Drop - the person on whom you make a thorn

Seller is the seller of the material needed by the carder

Driving in - entering information about the card when paying for the goods.

Staff - commodity

👆Chapter 1 - SS - Cardboard

CC - cardboard - all this means a credit card, but if we are talking about online carding, it is more likely information about the credit card and its owner.

👌example ss:

5571324761618000 | 1111 | 836 | Terrance Chan | United States | California | Alhambra | 91801 | 2226 Larch Street, Unit "E" | (626) 379-0768|terrychan@dslextreme.com

this is how a regular ss looks like, as mentioned earlier, this is information about a credit card and about the

owner, now we will write down what and where and what it means:

5571324761618000 - credit card number (16 digits)

1111 - card expiration date

836 - security code (CVV2)

Terrance Chan - name and surname of the cardholder

United States - the country of residence of the cardholder

California is the state of residence of the cardholder

Alhambra - city of residence of the cardholder

91801 - postal code (zip cod, postal cod) of the card holder

2226 Larch Street, Unit "E" - street and house of the cardholder

(626) 379-0768 - the phone number of the cardholder (optional) is not found on all ss

terrychan@dslextreme.com - cardholder soap (optional) is not found on all ss

This example of ss is very convenient and everything is clear on it, but it happens that a seller (seller of material) can give ss both in a bad format without divisions, and with unnecessary garbage, so I advise (beginners) to check with sellers before selling in what format they sell ss maybe even ask for ss for an example.

Before driving in, it is also important to know what brand your credit card is (MASTERCARD, VISA, American expres - the most common credit cards), you can determine this by the card number as follows. Remember:

if the card number starts with 4 - this is VISA, if the card number starts with 5 - this is MC (abbreviated

MASTERCARD), if the card number starts with 3 - this is Amex (abbreviated American expres)

Actually, owning this information, you can drive it into many services (skype, steam, online stores, etc.)

👆Add information

1. For MASTERCARD and VISA, the card number consists of 16 digits, for American expres it consists of 15.

2. The security code for MASTERCARD and VISA consists of three digits, for American expres it consists of 4.

3. Not in all ss the state can be written in full, very often it is indicated by two letters, examples: IA, AR, DE, etc.

4. Very often beginners confuse a city with a state in ss or simply cannot figure out where the city is, in this case, use Google.

5. The balance on a regular ss is never known. (there are special checkers, but there are very few of them, and most of them usually kill the card in 90%)

👆Chapter 2. Full cc and enrol

Full cc or as they popularly call them fulks - this is ss with additional information about the card holder, namely SSN, DOB, MMN

SSN - Social Security number (cardholder insurance number)

DOB - date of birth (date of birth of the cardholder)

MMN - mother's maiden name (maiden name of the cardholder's mother) (occurs not always, not required)

Here's an example of a fulka:

Shelby L Lawson 4217661367018157 0414 329 17408 Windcreek Circle Riverside CA 92503 United States 951-318-9331

DOB 01/13/1966

SSN 6647-303-7221

The following may also be present on the fulk: the cardholder's soap, the cardholder's phone number and the bank that issued the credit card (sometimes required when paying) But this can all be on a regular ss. The main advantage is information about SSN and DOB. What is this infa for? And what are the fullers themselves for?

They take fullers in order to make enrol, i.e. create a bank account. To create an account you need additional info (SSN and DOB). As a rule, cards are rolled in order to find out the balance of the card and get access to changing the billing address. And now what is all this for?

I think everything is clear about the balance (if not, there is a construction site ====>), but about billing - I think not to everyone, and it is even more unclear why it should be changed at all)) So, the billing address is the address of the card holder (i.e. home address, city,

state / region, zip code). The fact is that when registering in an online store, there are two such concepts as Billing adress (card holder's address) and shipping adress (delivery address). If they differ, then the order is checked more thoroughly, unlike the case when they coincide (the goods are sent within 2 hours)

Thus, for example: we have a USA shop and a USA ss, as well as a drop in the USA, we make a video, change the billing address of the cardholder to the drop address and then order the goods for the billing address and everything is ok))

But in reality, of course, not everything is so simple. It is not so easy to change the billing address, while at the very least you will have to accept the call and have the MMN info - and this is at least))

you shouldn't bother about Enrol - it's for general information.

👆Chapter 3. Additional protection of credit cards.

If you think that life is easy for a carder and that carding is a freebie, then you are wrong. Every day, bespectacled people in banks work hard to make life difficult for you and me. And then one day they came up with VBV - Verified by Visa. The essence of the system is that when paying for goods or services on the Internet, you must enter an additional verification code, which the cardholder receives from the bank that issued the card. However, this does not solve the problem of payment security. The problem is that the client cannot deny transactions that are not Verified by Visa protected. And even by paying only in those online stores where Verified by Visa is used, the client can easily steal data (card number, owner's name, expiration date, cvv2 code) sufficient to make legal payments on behalf of the client.

In short: VBV is an additional protection for visa cards (requires entering a password when paying) there are cards with and without vbv - some sellers (material sellers) check (check) on vbv. If you bought from a seller who does not check for vbv and it turned out to be from vbv, then such a card can only be thrown away. Therefore, check with the sellers.

As you understood VBV is additional protection of visa cards. The master card has a similar security called

SECURITYCODE. Credit cards of the American Express brand have nothing like this!

👆Chapter 4. Protection and anonymity on the Internet or fairy tales about the "K" department.

Oh, oh, oh)) I don't even know where to start.) I'll try to be brief and convincing. To begin with, I will write down the order of events after the order of any product, from any store. And so we ordered the goods from the store and they send it to us, then there are two options:

1. The cardholder does not lose money (the smartest option in this case, the purchase is completely legal and there is nothing to write here)) (by the way, this often happens if the amount of money is small or the cardholder temporarily does not have access to the card)

2. The cardholder fills the loss of money after some time (the goods have already been sent to us), then something like the following happens: the cardholder calls the bank, says this is how the money disappeared,

the bank tracks the last payments and says that this amount was debited for the purchase goods in an online store, the cardholder is all nervous, etc., says that he did not order anything and cries (my sick fantasy), after the proceedings (possibly long) - the online store makes a chargeback (refund of money to the cardholder) Thus, it turns out that the shop bears the losses. Perhaps, of course, there is still such a situation: the cardholder is a brainwave and will not be able to prove that he did not make any purchases and sew him and not the money back, for us this situation is also beneficial (I think it's clear, if not, then go ahead for the pills of iodomarin to the pharmacy), But let's return all the same to the situation when the shop bears losses. What happens next ?? There are again two options:

1. The shop clogs and then sells its junk (99% probability, because if the parcel leaves for another country, this is called the ends in the water, and if to india, then it is called the ends at the bottom of the world ocean - the Americans also understand this)

2. The owner of the store is a principled person, a veteran of the Second World War, etc. Such a serious Maine, of course, goes to the police station (to a regular police station, to a serious department for

combating cyber crimes with a statement about the theft of an electric kettle, he will not be allowed in) and so he comes to the station writes an application, the cops of course listen, but after when they find out that the kettle has left for Russia, they regretfully tell the "poor" store owner that it is more expensive to get involved with these psychos. and that's where it ends)

Perhaps some of you are not catching up with the simplicity of online carding. After all, you've watched videos on YouTube and read articles on how to catch carders. So: firstly, do not confuse real carding (they often catch in the ass there and successfully) and online carding (I don't know anyone who would be given for a thing for a period of time), and secondly, do not work on RU and CIS, here you are also very easy to catch. In addition, in 90% of cases, Russian carders are caught on the territory of other countries (again, they consider it useless to turn to Russian cops for help) Now about the "K" department. Who do you think works there ?? And there are former hackers and carders working there, who know that today there are several dozen small carders operating in india(who card for amounts from $ 2000-3000 per month), this is the same as trying to drink the Black Sea (my sick comparison). who poses a threat to our country (these are idiots who work on in) and serious guys who do from 10k per month. And this is not to mention bribes

and the fact that indian cops hardly imagine how to shop online with a credit card. And no one is caught for clothing carding)) and it's true.

Well, now after such a story, briefly about the methods of protection:

VPN - for the paranoid

Grandpa is the best option

Soks - if you use Dedicated files - are not needed!

So, why Dedicated?

The whole point of the thing comes down to the fact that the staff is sent to you as long as the cardholder or shop burns the setup.

That is, in order to be sent staff, you need to pretend to be a cardholder, to pretend to be a cardholder, for example, an American card, you need to have an American ip and an American computer

This is all provided by a Dedicated Server (remote desktop, someone else's computer)

how to connect to the Dedicated Server: Start> Run> mstsc> ip / Next, you will connect to the Dedicated Server and the account window will appear (with the login and password input)

Here is an example of a Dedicated Server: 216.85.236.42@Administrator; p0o9i8

And so: 216.85.236.42 is the ip address of the remote desktop

Administrator - account login to connect to the remote desktop account

p0o9i8 - account password for connecting to the remote desktop account

Once again I repeat how to connect: click Start, find the Run button in the menu, or (white field at the

bottom) - enter the command: mstsc - then start the "Remote Desktop Connection" program ..

in the free white field of the window, enter the IP address of the Dedicated Server and click to connect. (A window about the security of the connection can come out: click YES!) Next, you connect to the computer and a window with data input from the sites is displayed.

There you enter your username and password and click connect (or there will most likely be in English). Next, the desktop of someone else's computer should appear.

Chapter 5. Drops

Drop - the person to whose address you make a spike. Personally, I advise you to resort to the services of a drop, in the event that the shop does not send to your country, now there are few shops that send, for example, to India , in which case carders are looking for drops, for example, in yus and make spikes on them - this increases the likelihood that the product is successful will be sent. And if you have a store that sends to Russia, then you can send it calmly to yourself

(as all normal people do), if you do not trust my experience, you can create a topic for discussion. You should resort to drops in india if you work on indian, i.e. you hiss from indian stores and onto indin cardboard (but I only work on india), so see for yourself.

To better understand why drops are needed, consider two situations:

1. You have a USA cc + USA shop, you order the goods to india or any other(the probability that the goods will be sent is small) - (although there are many such shops now)

2. You have a USA cc + USA shop, you order the goods to the address of the drop who lives in the USA (the probability that the goods will be sent is high)

Now I think it became clear to you that they are looking for drops not so much for safety, but as for a successful drive.) You should also know that there are two types of drops

Adjustable wedges (a person does not know that he is working for a carder, such drops are often caught)

Not adjustable (a person knows that he accepts a carved product, observes safety measures, etc.)

👆How to find drops?

In general, there are special people called drop drivers, they have a certain amount of drops. You can work with drop lines in different ways, for example: the drop line gives you the drop address, you make a spike on it, after which the goods are sent to you in india (for%), the second option: this is when the drops sell the loaded goods themselves, i.e. The drop guide can immediately pay you on the track or after the sale of the goods, there may be more options.

You can search for drops yourself, if you speak English, then go ahead to the forums where Americans are looking for additional earnings))

👆Chapter 6. Breaking through additional credit card information

First, a few definitions:

Issuet bank - the bank that issued the card and controls it

Bin - the first six digits of the card number, which can be used to determine the following: bank issue, card type, card level, card brand. How to punch through information and how it looks like I'll tell you now:

1. Go to the site bindb.com

2. Press SEARCH BIN (above)

3. Enter bin and captcha, after entering press Search

after which information should come out like the following:

Bin: 421766

Card Brand: VISA

Issuing Bank: BANK OF AMERICA NATIONAL ASSOCIATION

Card Type: DEBIT

Card Level: PLATINUM

Iso Country Name: UNITED STATES

Iso Country A2: US

Iso Country A3: USA

Iso Country Number: 840

Why do you need this information? Information is the most important weapon of a carder, in carding everything revolves around information, roughly speaking, the more you know, the better. Issuing Bank (bank issuing) sometimes requires when paying, Card

Level (card level) depends on the card's fatness, the higher the level, the more likely it is that the card has a large balance. In general, you can extract a lot of useful information from any information))

👆Chapter 7. Shops

I think the chapter about shops is the most important. Why? I'll tell you now. The fact is that many beginners think that all carding is directly driving it in. But driving it in is easy and not difficult (stupid filling in the fields). It would be safe to assume that this is all carding. In fact, there is a lot of tedious and boring work in modern-day carding. Let's figure it out. And so we have ss + Dedicated, but where to drive in? Where can I get a shop that can be easily sent? To drive into the first shops that come across is nonsense) First, let's introduce a few more concepts that you need to know before "going to the store"

1. Billing address - Billing adress (alt. Payments information) - cardholder's address, ie. billing address

2. Shipping address - Shiping adress (alt. Delivery information) - delivery address, ie. your address or drop

Now, in fact, we will learn to identify POTENTIALLY slutty shops (i.e. shops in which it makes sense to try to drive in). To do this, go to Google and drive in various requests (I think it's clear that in English) and browse online stores. And now a few nuances that need to be seen in order to understand whether this shop is right for us:

1. The shop must accept a credit card for payment (if you do not see the credit card symbols in the store, such a shop can be discarded immediately)

2. The shop must be sent to a separate from the Billing adress (ie, there are shops that are sent only to the cardholder)

3. The shop must also be sent to the country we need (for example, not all shops are sent to india)

4. Is there a delivery method to india (it often happens that india is on the list of countries, but there is no way to deliver there)).

But only when all these points satisfy your situation, only then you are already driving. (via Dedicated, well, that's all)). But the best way to determine these nuances is to emit them, i.e. you stupidly go to the website of the online store: choose a product - register (all data on the ball) - well, then you go to the payment itself, looking and defining everything that is written above. Thus, you select a certain number of shops and then you already make real drives in them)

And now ATTENTION! I repeat! And so: to find out whether the shop is sending or not is IMPOSSIBLE without driving it into it !! But this does not mean that you need to drive into the first shops that come across .. For this, we first look through the shops on our computer (i.e. hang out there as an ordinary visitor - register - we reach the payment and simultaneously look at all the nuances) - what are the nuances we are interested look above! Of course, it is possible and not necessary to constantly register, because "bad shops" can be immediately identified (from pictures, etc.) - but I insist that you jerk off your claudia and your eyes,

because there is no place without these nerd skills. .
CARDING IS NOT A FREE SHIP.

👆Chapter 8. Additional information before driving. (nuances)

And so we have already figured out that driving is nothing more than a regular payment (only from someone else's account) .. Now let's look at the minor nuances that can positively affect driving ..

If you think that by buying a grandfather and ss (valid) you will succeed 100% - this is a delusion))

And so we will analyze the points:

1. Grandfather and ss should be selected necessarily from one country and preferably one region (region, state)

2. It is better to drive in before lunchtime (local time dedik)

3. The most favorable days for driving are Monday, Tuesday and Wednesday.

4. You cannot order several times from the store to the same address !! (Just kill the shop)

3. It is better to use 1 ss for one drive (if you have not driven into one shop, you can try to drive into another, but after a successful drive, it is better not to touch the card anymore !!)

4. If you order goods to one country, and pay with a card of another country, then most likely nothing will work for large amounts .. (For example, you have a USA ss, and you order the goods to india, in this case I advise you not to make the order amount more than 250 $)

5. And in general, remember: the smaller the amount - the more chances that they will be sent.

6. Payment for delivery is also included in the order amount, so you can save on it .. (do not choose the fastest way, choose the cheapest one)

👆Chapter 9. Practice (driving into the shop)

And so for an example of driving in, we take:

1. Dedik 66.158.172.131 (IP) xerox (login); xerox (password)

2.CC 4782002000276404 0612 721 Rene Gonzalez 1381 Belle Haven Dr. Grayslake IL United States 60030 6093971415 JPMORGAN CHASE BANK NA DEBIT DEBIT CLASSIC UNITED STATES

3. Online store mp4nation.net

Hmm, and so! First of all, we connect to the Dedicated Server ..

Next, select the product

Next, click add to cart (this means putting in the cart)

Next, click on the chekout button

Next, click sign up (registration), then the registration window should open)

We fill in the data from ss .. your soap must be registered in advance (soap must be Western services, yahu, etc.) on the soap you will receive information on the following (for this do not * beat it, etc.))

after everything is filled in, press sumbit:

pay attention to the inscription shiping adress (this is the delivery address, i.e. your address), as you can see, the store by default filled it with the same address as the cc address .. Therefore, press change adress and edit ..

also pay attention to the inscription shiping method (delivery method)

press continium chekout:

then a page with billing information opened - billing address, order amount, and here below we select the

payment method .. (credit cart), here you also need to indicate the brand of the card with us a visa ..

Also, be sure to check the box: I have read and agreed to the terms and conditions bound to this order. This inscription is always there (look for it on the page)

how we did everything, click on (chekout), after which we should open the last page - which contains all the information on the purchase .. I advise you to check the addresses again (shipping and billing) Remember: Shipping address is the delivery address, and billing address is this is the billing address (address with ss)

Click confim:

As you can see, we were transferred to another site (this is called merch) - a special computer that almost any online store has - it will process your order .. and determine whether it is accepted or not .. here we enter the data ss (number, date and cvv)

Click Make Payment:

Merch sent me to fuck!))) As you can see, having done everything right - there is no guarantee that everything will work out))

In my case, the reasons for the failure are most likely the following:

1. Not valid, old ss

2.Dedicated state and SS state are different

3. The shop which took place after driving, has long been public and cost ** n

👆Chapter 10. After a successful drive. What's next?

And so: let's say we did all the rules, the payment in the shop went through (i.e. the card was hammered in), what's next?

I will say right away that this does not mean a fig. Those. not the fact that the goods have already been sent 100% .. This only means that your order has been

accepted for consideration, and people will already be considering it.

All further information about our order will go to our soap (which we indicated during registration). If you have problems with English, I advise you to use a translator .. But as a rule, standard letters come to the mail ..

The types of letters are as follows:

The first letter is most likely a notification and gratitude about registration on their website

The second letter is a notification that your payment has been accepted and will soon be considered (this is called an order). If it didn't work for you, then most likely they will also send a letter with the opposite content.

But the options for the third letter may be different:

1. A good option! You will be sent a letter that your goods have been sent or will be sent soon .. (this is

called "hurray track given") Track is the number of the parcel by which you can track its position in the flesh before arriving in your city. By the way, a parcel can be sent to you without this track .. (depending on which delivery method you have chosen), as a rule, the cheapest methods are sent without a track number.

2. Semi Sad option! You will be sent a letter in which they ask you to prove the fact that you are the legal cardholder .. (You may be asked for a photo of a credit card or its scan or a scan of some other document, I can also ask you to call them and confirm by phone again the fact that you are a cardholder) .. On the carder forums there are a lot of services that draw scans and receive calls, I really hope that such worthy services will be here over time.

3. Bad option! There is nothing to write here .. A letter will come in which you will be sent to heaven for an asterisk.

👆Chapter 11. More about parcel delivery

Here I will try to describe everything about deliveries.

Go. In general, there are three main delivery services, these are:

DHL (almost all over the world), EMS (almost all over the world), USPS (USA) ..

In general, in order not to paint a lot, I will say right away that I advise you to punch the track here: post-tracker.ru/

But here the information will start to appear if the parcel is already on the territory of the Indian Federation.

track-trace.com/post - track a parcel by order number around the world from almost anywhere in the world - 97 countries are here!

👆Chapter 12. Frequently asked questions. And contacts of sellers.

1.Question: Is it possible to buy ss and withdraw money from it to the VM

Answer: Theoretically possible, but if you start your activity from this, you will fail! In general, on a straight line from a regular ss, you will not bring anything anywhere)) And the schemes that are sold, such as CC => VM (on * ball)

2. Question: The package has arrived. How to get it. Stupid to go to the post office and that's it?

Answer: YES! Most likely you will receive a notification - you fill it out and go to the post office (I can ask for another passport at the post office)

3. Question: How to find out the balance on ss

Answer: Nothing. (that's why they cost so little, because sellers are not responsible for the balance

Finally:

Never get involved with activities in india. (In general, not at all) If they catch it, it will be too late ..

👆👆Vocabulary Nutshell👆👆

Authorization - checking and defining the authority to perform certain actions. Permission granted by the issuer to conduct a transaction using a bank card. During the authorization process, data about the card and the requested amount are transferred to the issuing bank, where the status of the client's account is checked.

Account (acc, account) - account.

AmericanExpress (AmEx) is an international payment system, the card number starts with 34 or 37 and consists of 15 digits.

ATM - ATM - a tamper-resistant bank security device designed for: issuing and receiving cash; preparation of documents for transactions using bank cards; issuing account information; making non-cash payments, etc. The ATM is equipped with a processor,

display, keyboard and reader designed to read information from the card.

BIN - the first 6 digits of the bank card number, which determine the bank that issued the card and its type (classic, gold, etc.).

Card number - card number - a unique set of numbers applied to the card as a result of embossing, as well as stored in memory on a magnetic stripe or in a microcircuit.

Card owner - the cardholder is the organization that issued the bank card.

CVV (Card verifikation value) - the verification value for the card number is in the dump.

CVV2 - additional security code, located on the back of the vehicle, usually consists of 3 digits.

DL (driver license) - driver's license (English).

Expiration date (exp. Date) - the expiration date of the card, it is on the card itself and in the dump.

VISA is an international payment system, card numbers start with 4. Site.

Western Union is an international money transfer system.

Wire transfer - bank transfer.

Gold credit card - a gold credit card is a prestigious payment card that provides the holder with priority status, a high credit limit, automatic insurance and other privileges.

Debit (debit) card - a card that can be used only within the limit of the amount available on the account.

Drop is a person who takes on (consciously or unconsciously) the dirty part of the job. Accepts money transfers, provides an account for transactions by other people, etc.

Carder is a person who uses information from someone else's bank card to receive money.

Carding - getting money by using information from someone else's bank card.

Cardholder - a bank card holder, an individual or legal entity.

Ripper - a person who threw someone from the carders.

Credit card - a card that you can use to buy on credit, i.e. not having enough money on the account. The amount of the loan is determined by the issuing bank.

MasterCard is an international payment system, katr numbers start with 5.

Soap - E-mail, e-mail address.

Cash out - converting virtual money into real money.

PAN - bank card number, most often 16-digit.

Payment system - an association of banks and companies operating according to the general rules for the use of cards. The basis of the payment system is a set of regulatory, contractual, financial and information-technical means, as well as decisions of the participants, which regulate their relationships regarding the procedure for using cards. There are several membership statuses in the payment system: full, partial, etc. All cards that belong to one payment system have signs that allow identifying their belonging to this payment system.

Prepaid card - a prepaid card - a smart card that stores electronic money prepaid by the cardholder.

Scan - scanned document, photo, bank card, etc.

Transaction is a banking operation consisting in the transfer of funds from one account to another.

Use - use.

👆👆Internet carding.

Adult (adult) - a porn site, or in general a site with content for adults.

BidPay is a payment system that allows a person who bought something at an auction to pay for their purchase. This is a payment system that allows you to make MO without any problems using a card.

Billing is a payment system.

E-gold is an Internet payment system.

Internet carding is the use of data from someone else's bank card to carry out all kinds of transactions on the Internet in order to receive money.

Card (cardboard, potatoes, CC, SS) - bank card number. Used for online shopping. Happens with and without cvv2 code.

Merchant - a trading account that receives money for a sold product, an online trading system.

Stick is a PayPal money transfer system.

A proxy is a server function that allows a user to work on his behalf.

SalesCart is an e-commerce package integrated with Microsoft FrontPage to enable online shopping.

Socks (Socks-proxy) - an intermediary server between your computer and the final site, used to hide the IP.

Spam is a large-scale distribution of letters by e-mail.

SSN (social security number) is a number given to every resident of the United States for the most convenient taxation and tracking of credit history.

DOB - date of birtday date of birth

MDOB - Mother date of birtday

MMN - Mother maiden name mother's maiden name

MPOB - Mother's Place of Birth

Chargeback is a withdrawal by a bank (cardholder) of a payment in respect of which there are doubts.

Enroll - connection of a credit card (account) with an online connection with the ability to recognize and change data via the Internet.

IP - Internet address, consists of four numbers separated by periods, each of which can be from 0 to 255. Identifies the user's location.

Common abbreviations.

Acc, Acc - account.

Amex - American Express.

CC - Map.

CVV - Card Verification Value.

DI - driver licenze.

Exp. date - Expiration date.

KK - card.

MG - Money Gramm.

MO - Money Order.

PIN - personal identification number.

SSn - Social security number.

WM - WebMoney.

WU - Western Union.

What is Enroll cc, this is a ss with access to a personal account, where we can see the balance of the card, change the billing address of the kx, change the phone number to our own, make a transfer of funds, accept minikis, link vbv.

Minikis - mini-deposit, writing off a small amount, to authorize your ss / ba in payment systems / sites / platforms, in a secure way. If you take minicas any place where you take that is bad, it will be more loyal to you. Minikis run 2-3 business days (weekdays).

You can drain Enroll ss to cashiers. After enroll you can check the account. More details will be discussed in the ba. Further, from there it is already to drain money.

To upload ss you need to do the following

1) Buy ss, debit or credit without a difference. Depends on the bank. We do not take the top bank. Where to break the bank you have.

2) Next, we punch to ss ssn and add, perhaps they will require more mmn and mdob. MMN - mother's surname, MDOB - other mother. MMN and IDOB can

be found in the archives http://www.archives.com as well as ancestry.com (only states of America -

FL, OH, CA, ML, TX). Punch similar sites in countries and look there. Or, with the help of SI, we hollow it into mail / facebook. We check through people com.

The cases of MMN and MDBI are best put aside. Reach ssn + ext, break through bin and take this bank! There are many such banks.

If mmn + mdob, you can also refer to the punches.

All punches, etc. will appear under the hashtag.

Go to the bank's website, click Enroll here / Enroll. If the video is already filled in 40-50% of cases, they require ssn + ext.

They may also require the login of an existing personal account or BackGround (questions like the color of the car).

To find out the login, you can do the following - introduce yourself as a bank and send an authorization letter (si) to the mail, or try to enter options like name kx and his birthday (pAul93). The situation with BG is worse, but we can break through the BG ourselves. How to do this will be broadcast on Skype. In such cases, they may also request a place of

work, work phone number, etc. I advise you not to dig into this at the beginning. BG can be pushed to intelius checkmate whitepages.

If not, we enter all the info of the card, ssn + ext, the soap you made under the kx, and at the end the answers to secret questions (BG). Come up with them yourself and ok.

You have gained access to your personal account.

Sometimes they require a phone number to receive SMS, in this case you need a gv or a real number. Gv- Google Voice.

We take grandfather under the ip ss. Spam mail immediately after enroll.

Actions after enroll:

1) Disable Message & Alerts in any case, give a lull for 1-2 days. So that sms do not come to kx.

2) We change the phone to our own (if the phone is already tied up) in 3-7 days, depending on the bank. Sometimes it even takes 30 days. It is best to keep the phone unavailable.

3) Change the billing address to the middle or drop, you can immediately after the first point. In this case, you can beat the bill = thorn, the next day the billing changed. You can try right away.

4) See if it is possible to create a checking account.

In your personal account, you can tie up vbv (not in all banks). Or tie up vbv on off sites visa / mastercard / amex. Vbv will be good at exchangers / hotels / air. We will analyze in the future.

The following cans are easy to roll at the moment:

1) Bank of America 2) 1st National 3) US Bank.

Roll on ssn and ext.

Bank of America - you can deposit this bank (rolls easily, but a lot is overloaded). Further, in the bank itself there is a Visa Checkout. Go there, change the billing in the visa itself to your Shipping (where you send the goods). Then we go through the configured android into Valmart and hit through the visa checkout (enter the log and pass from it). First, 200 bucks, then 800. Etc .

You can also upload US BANK. https://www.usbank.com/index.html. Next, completely squeeze the account and make a Checking account out of it. Will be in lectures on BA. We don't

even think about that yet. US BANK also rolls on ssn and ext.

In general, if an account falls into the limit, then it's better to forget about it, right? How annoying it can be, a decent amount remained on the balik code ...

The main limit that we most often catch (in my opinion and my statistics) is medium, usually for withdrawing a medium, they ask for this data: Confirm a bank (to confirm the bank) or Confirm a card (to confirm the card)

Confirm identity (accept SMS or call to the number tied to the stick) or Provide proof of your address (confirm the address) or Upload a photo ID (passport or license) or the stick asks to add security questions and change your pass.

In the stick, the limits must be removed from bottom to top, that is, first we change the pass, then add the secrets

Next, go to Confirm identity (receive an SMS or call to the number tied to the stick) or Provide proof of your address (confirm the address) or Upload a photo ID (passport or license) here you need to send one stick. Since almost every stick insect uses a google voice, we'd like to choose the first confirm identity option. It is unnecessary to paint anything, since it is stupid to

receive the SMS code and then all 3 checkboxes will be confirmed. Recently, the following problem has appeared. When you click on confirm identity, we see that we cannot receive SMS and the option remains Provide proof of your address (to confirm the address) or Upload a photo ID (passport or license)

here, as you already understood, we approach drawing. Which costs money ... well, I found a trick to work around this error.

To do this, we follow the link https://www.paypal.com/webapps/authmessaging/authflow?execution=e6s1

Next, we receive SMS, which is sent without errors, and voila, we bypassed the confirm identity.

Further, there are such items for removing the limit as:

Confirm a bank (to confirm the bank) or Confirm a card (to confirm the card) as we use the BA. then it will be the BA that will be verified. By default, the stick asks you to verify the bank that was previously attached, but you need to verify it with mines.

In most cases, if the stick requested a BA verification, then the log and the pass on it have already been changed, so verifying with mines is not an option. To do this, we take ANY OTHER bank, attach it to a stick and thereby confirm a bank with us)

We can consider the stick as limited.

If it suddenly happened that you could not remove any item yourself, and after drawing the docks, sent it to a stick and at the same time after 2 days, the limit is not removed, then be sure to order a ringing!