Carding Guide, All My Knowledge

Written by Alpha02, VIP @ TCF, May 17, 2014

Introduction

This guide was written by Alpha02, VIP at TCF, after a long list of requests for making a guide. I'm an experienced carder, carding tens of thousands of dollars worth of merchandise and rarely failing. I share my knowledge for anyone who is ready to put a bit of money on the table and get some real up-to-date carding information.

Now, at the time of writing, I am the only one allowed to sell this guide. If you see anyone selling my guide on EVO or anywhere else, let me know. I took time to write this guide, I appreciate when people recognize my work.

So, let's get started!

Table of Contents

Introduction
Chapter 1 – Virtual Carding
1.1 – How It Works
1.2 - Account Take-Over Fraud
1.3 - Why Orders Get Canceled
1.4 - Drops
1.5 - Chargebacks
1.6 - Warranty Fraud
1.7 - Picking The Best Cards
1.8 - Commercial Fraud
1.9 - Newegg And TigerDirect
1.10
– Stripe Cashout
1.11
- Beyond the ATO – The PTO
Chapter 2 – Protecting yourself
2.1 - Protecting Yourself Online
2.2 – Burner Phones
2.3 - AVS
2.4 - Flight Tickets
2.5 - Glossary

Chapter 1 – Virtual Carding

This chapter is about virtual carding. Virtual cardung is the art of ordering goods online using stolen credit cards, also known as “CVV”, “pizza”, any any other names the members of the community use to disguise their intentions. Although this seems easy, there are many pitfalls you might want to be aware of when doing that, especially since merchants are getting more and more aware of online fraud. Want to know how to get free goods? Let's get started!

Section 1.1 – How It Works

The first thing is to ask yourself, how much do you want to card, and what do you want to card? Then, you will have to pick one of those 3 levels. Each level represents a difficulty level and you will see the prerequisites.

Level 1: Easy carding

This level is used for very easy things to card, for example restaurants and small phone orders, mostly under $50. This is the entry point of most carders. For that, you will need:

- Credit card number
- Expiration date

Level 2: Intermediate carding

This level is used for online transactions that are slighly higher, like background reports, or a very small physical item. You will need:

- Credit card number
- Expiration date
- CCV code
- Cardholder name
- Full billing address
- Sometimes, phone number of the account

Level 3: Hard carding

This is not recommenced for beginning carders. Here we are talking about everything above level 2, such as large physical items, or high-security websites like Newegg, TigerDirect, and sites that require Account Take-Over (for ATO, see section 1.2 of this guide). Computer parts, electonics, and many other items fall in this level. You need:

- Credit card number
- Expiration date
- CCV code
- Cardholder name
- Full billing address
- Phone numbers
- SSN
- DOB
- Recommended, background report

If you are aiming for level 1 carding, you just need to call for pizza and order pizza to another address, no need to write lengthy paragraphs on this one. This is easy and is pretty straightfordward.If you are aiming for level 2, you can card background reports or small physical items, mostly under $150. All orders are done online, and you will have to enter the correct billing address, shipping address, and card information.

Now, you must see if the websites says billing phone number on file with the bank, or simply contact phone number. If the website asks for billing phone number, you have to put the phone number on file with the bank for the cardholder, otherwise it is safe to put your burner phone number (see section 2.1 of this guide). Now, is the website going to call you? It depends on the order, their policy and their suspicion about you, so there's no safe answer to this question. Remember that carding is often trial and error.

When you use a card to hit a website, do not hit another website using the same card until your order has shipped. Making an order go though and having a charge approval is easy, but getting it shipped is often where the challenge lies.

A level 2 site that is often carded is peoplefinders.com. This is where carders get most of their background reports. It is a good playground to test your skills, and will prove useful later.

Now, on to level 3. You probably saw the information required, now how to get it? First, if your subject is aged under 40, chances are that you are out of luck. Otherwise, read on.

First, you need to get the right type of card. This is called finding the right BIN (Bank Identification Number). The BIN is the first 6 digits on the card and is used to identify the card type as well as the issuing bank. To learn more, go to bindb.com, at the top go on Bin Search, and enter the first 6 digits of the card. They will tell you the issuing bank, and card type. You have debit and credit cards, and the card type can vary. From the weakest to the strongest, they are:

- Secured: Very low limits, sometimes around $300
- Classic: Low limits, sometimes around $1000
- Gold: Average limits, can be around $3000
- Platinum: High limits, can be around $8000
- Business: Very high limits, in the 5 digits, often around $15,000
- Signature: The best ones, I got cards that had $30,000 of credit limit

Note that those numbers are subject to change according to the cardholder's credit score, history, and spending patterns. For the benefit of this guide, we will only work with credit cards. By experience, debit cards often do not have funds, and have tighter security for online purchases. In other words, they are rubbish for level 3 carding, but may have other uses, like level 1 or level 2 purchases.

Register an account on any SSN finder site such as ssnfinder.ru or ssndob.cc and look for your subject. At the same time, go on peoplefinders.com and get the full background report of your subject using a level 2 card. Once you have the background report, look if the addresses and date of birth match on the report and on backstab. If everything matches, you can assume the SSN will be correct. Use your common sense to compare the backstab and peoplefinders results to make sure you didn't get the wrong information. About 80% of the subjects over 40 years old can be found.

You have the SSN and DOB? Great! Now, time to get the mother maiden name. This is slightly harder and will work if your victim is in one of those states: Arizona, California, Delaware, Idaho, Indiana, Kentucky, Maine, Maryland, Massachussetts, Minnesota, Nevada, New Hampshire, New Jersey, Ohio,Rhode Island, South Dakota, Texas. Go on archives.com and card an account, then look for your subjet's mother (look at the background report for her name and date of birth), and try to look for her birth record. This is a trial and error case and works about 50% of the time.

Why get all this information? Because many level 3 swites will have either VBV (Verified by Visa) or MCSC (MasterCard Secure Code) protection during checkout. This is a form that is presented by the issuing bank of the credit card and asks for additional questions. Although every type of card is different, the commonly asked questions are:

- Date of Birth
- Last 4 digits of SSN
- Full name on card
- Billing zip code

If you fail any of those questions, the order will not go through. Now, why did we need all this information? Because we will perform a ATO on the account. This is tricky. Read the next section for a detailed description of Account Take-Over fraud.

Section 1.2 – Account Take-Over Fraud

Do you dream of carding thousands of dollars worth of computer hardware on Newegg? It's doable, but not easy. You have to follow the right steps. I carded a $10,000 gaming rig in under 2 weeks using platinum cards by following that guide, so I'm in position to tell you how.

First thing, check the balance of your credit card. Now, before going crazy, remember this rule of thumb: Do not use card checkers! They burn the card very quick. Let me explain.

Every transaction automatically gets a fraud score between 0 and 999. The system used to evaluate transactions is the same used by the big 4 banks and is called Fair Issac. Transactions having a fraud score over 300 will hit manual review by an agent, who will decide if they contact the cardholder or just let it though. Scores over 500 with auto-decline, block the card, and an agent will contact the cardholder. Some banks have different criterias, but things that can affect the fraud score are:

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

For example, a $20 charge in the cardholder's local Walmart will not trigger anything, but a large purchase of $2000 on Newegg.com will have a high fraud score and probably auto-decline if the cardholder rarely makes online purchases.

So how is this relevant? A small card-not-present charge followed by a big charge will make the fraud score very high, because they assume you are testing the card. If they see a small $1 charge, then a few minutes later a large purchase online, they will auto-decline the card and your plan will likely fail.

There are much better ways to check if a card works. The best way is to call the bank's toll-free number and use the automated prompts. This brings no danger, however use Spooftel to spoof your number to display the cardholder's number. Once you do that, you are ready to call the issuing bank's number and check how much is left on the card. Let's get to it.Call the bank using your burner phone and have in hand the following information, according to the bank. The automated prompt will give you access to the transaction list, balance, and a few other options. Here is the information for the biggest 4 banks:

Chase Bank – 1-800-432-3117

- Full card number
- Zip code

Note: If you correctly spoofed the phone number, you will only be asked for the last 4 digits of the card, otherwise you will be asked for the full card number.

Citibank – 1-800-627-3999

- Full card number
- Last 4 digits of SSN

Bank of America – 1-888-421-2110

- Full card number
- Zip code

Capital One – 1-800-955-7070

- Full card number
- Last 4 digits of SSN

If, for any bank, you enter the card number and the system immediately transfers you to an agent without additional questions, it means the account is closed and the card is burnt. No need to waste time on this one, just hang up and use another card. The agent will only tell you the same thing, and you will look dumb.

It's always a good practice to take note of the last transactions and amounts, just in case you get asked for them later. Listen to them and write them down, I recommend up to 8 transactions for maximum safety.

So you have the balance and the available credit line now. Nice! So you know how much you can spend online. Before you go crazy though, there is one more obstacle you need to be aware of: many sites like Newegg or TigerDirect refuse to ship to an address that is not on file with the bank. And chances are that your cardholder does not reside at your drop address. Here is how we will solve this problem, introducing the Account Take-Over fraud, also known as ATO.

ATO is the process in which a fraudster (you) calls the bank to make whatever changes he wants to the account, without the cardholder knowing. This involves speaking with a customer service agent and using social engineering. Before you even think about pressing 0 to speak to an agent, make sure you have, at the very least, the following information in hand:

- Full card number, expiration date, CCV code
- Full billing address of the cardholder (and county)
- Date of birth (and write down the age too, not just the DOB)
- SSN
- MMN (Mother Maiden Name)
- Employer name (facultative, if possible, try to find it on Facebook)•

•
•
•
•

Car make and model (facultative, if possible, try to do a Google StreetView on the CH's house)
House size and value (facultative, if possible find it in realestate.com as this is public information)
Driver's license number, expiration, state (facultative)
Previous addresses
Background report

In case you do not have the MMN, try to guess using common last names in the background report. If you really cannot find it, sometimes it is possible to get around it with other questions. Once you have this information in hand, study it, try to remember it. Remember, you are the cardholder, the card is yours, and you are confident, just like when you call your own bank for a legitimate request.

When you call the bank, you will be usually asked for 3 security tokens. Those tokens can be, but are not limited to: DOB, SSN, Address, CCV code, cellphone, MMN. If you fail 1 token, you will be asked 2 more. At this point, 2 things can happen:

1. You did it correctly, so the agent will listen to you and will do whatever request you have to do on the CH's account, and no flags will be raised.

2. The agent suspects an ATO is occuring, and transfers you do the securiy department. This is called the Verid department, and you will be asked 2 OoW (Out of Wallet) questions. Those are multiple-choice questions based on the cardholder's credit history and public records. They can be easy or tricks, it's random every time it happens. If you fail those, they will tell you that they can't help you and will suggest you show up in person at your bank. They will also ring the cardholder. So if you fail this one, forget this card, it's burnt to a crisp.

The first thing you want to do on the account is change the billing phone number. Only that. Do nothing else, as making too many changes will raise a red flag on the account. Call to change the main billing number and let the card sit still for at least 5 days.

All right, are you ready? Relax, sit in your favorite couch, call the bank, listen to the prompts, and press 0. The message goes on, this call may be recorded for quality purposes.

This is the first example, if you have the correct MMN (this is the most frequently asked token).

Agent: Thank you for calling Chase, my name is Bob, who am I speaking with?

You: James R Layton.

Agent: Thank you mister Latyon, and for security purposes, may I have the mother's maiden name on the account?

You: Lucile.

Agent: Thank you, and what is your date of birth?

You: October 1 st , 1965.

Agent: Thank you mister Layton, what can I do for you today?

This is the second example, if you do not have the MMN. Guess it, and do not hesitate. You know yourself better than the agent does, and they can only rely on the information they have on their screen to validate your answers.

Agent: Thank you for calling Chase, my name is Bob, who am I speaking with?You: James R Layton.

Agent: Thank you mister Latyon, and for security purposes, may I have the mother's maiden name on the account?

You: Smith.

Agent: I actually have something different here, it starts with C.

You: With C? It's impossible! Her name was Lucy Smith, she never used any other name!

Agent: Well, you do not have any other name that might start with C?

(if you have a last name starting with C on the background report)

You: My aunt's maiden name is Charlotte, but I doubt that's the answer you have on file.

(if you have nothing like that on the report)

You: No, no one in my family uses such a name.

Agent: Oh well, let me take note of this for you, can you confirm the last 4 digits of your social security number?

You: 4456.

Agent: Thank you, and what is your date of birth?

You: October 1 st , 1965.

Agent: And you billing address with the zip code?

You: 123 Fake Street, Fakeville, NY, 10008.

Agent: Thank you Mr. Layton, how can I help you today?

If you hear that, it means you got in. Otherwise, you will be transferred to the security department for the multiple-choice questions, have your report in hand. If you fail, the card is dead. Make sure you spoofed the cardholder's number, otherwise you could be asked for other questions like driver's license number, vehicule plate number, etc. Those are questions you probably do not have the answer to.

Now, what you want to do is change the billing phone number. A sample dialog with the agent can go as follow.

You: I would like to change my phone number. This phone will be disconnected tomorrow and I want to give you my new primary number so you can reach me if there is something.

Agent: Okay I see, what is the number?

You: 234-567-8901.

Agent: Thank you, is there something else I can do for you?

You: No thanks.

Agent: Thank you for calling Chase, have a wonderful night.

Once you passed the verification part, the rest is pretty straightforward and is relaxing. Now that you changed the billing number, let the card rest for at least 5 days. Do not make any transaction. The cardholder will continue to use his card normally too. During your call, at the end, if you failed the MMN question, you might want to remind the agent to change the MMN on file to avoid problems next time you call.

Also take note, at any point, if the agent wants to put you on hold, or says he needs to verify something and will be back, wait for him to put you on hold, and hang up. It basically means they are going to ring the cardholder. If this happens, you might want to wait at least 48 hours before calling again, and you will see just by the automated prompts if the card is burnt or not. Maybe they did not call the cardholder, but in 90% of the cases, they did. It happens, especially with Citibank, who likes to replace the Verid questions by a quick ring to the cardholder.The questions often change when you call, but they always follow a certain pattern. By experience, I will give you the tokens usually asked by the big 4 banks, but we aware that they might change, or they might ask you other questions if they believe you are bogus. They can ask for your age to throw you off, as you might not have to calculate it fast enough using the DOB. If you fail this verification, you will be transferred to Verid department.

Chase Bank, level: hard

- Full name
- MMN (if failed, last transaction)
- Last 4 of SSN

Citibank, level: medium

- Full name
- Password (pet name, MMN, favorite hobby, or best friend, if failed, last 4 of SSN and CVV)
- Mailing address
- Phone number

Bank of America, level: easy

- Full name
- (sometimes) Verbal password, which is MMN (if failed, DOB)
- Last 4 of SSN

Capital One, level: medium

- Full name
- Last 4 of SSN
- MMN (if failed, DOB and mailing address)

Since you have to wait 5 days, it's a good idea to create an account on your target website, browse the items, put some in your cart, go to checkout, go back, remove items, read descriptions. Just try to appear like a legitimate shopper. Remember that $1000 is a lot of money for the average American and if you show you don't care about your money and just throw items in your cart, you raise flags. Look like you care about how much it costs.

Once you got rid of this verification process, it will be easier next time you call the bank for this account. So let's suppose you followed me and let it sit for 5 days. Call again, and this time, we will add a temporary shipping address to the account. A transcript can go as follow:

(pass verification questions)

You: I want to make a purchase from Newegg.com but they ask me to add a temporary shipping address on file. I'm not sure how that works, do I just tell you where I want them to send my order?

Agent: Let me help you with that, we can add an alternate address on the account, what would be the address?

You: 123 Fraud Street, Cardingville, CA, 98765.

Agent: No problem mister Layton, I have notated the account for you, is there something else I can assist you with today?

You: No thank you

Agent: Have a good afternoon.Almost all banks allow that, except Bank of America, who can only change the mailing address. That's why their cards are not the best when it comes to level 3 carding, but some stores will do a conference call with the bank to bypass this restriction. Chase works the best for temporary shipping addresses, but is hard to ATO. It all depends on your skills and what you're comfortable with.

Once you have added the alternate address in the account, it's time to make the hit. Take your account on the website you want to card, shop a little bit again, then proceed to checkout. Try not to go over $2000 per order. Enter the correct billing address, double-check the information. Enter the billing phone number (the one you added on the file at the bank), then your shipping address. Triple-check all the information for accuracy.

Then, send the order. You might be greeted by a VBV or MCSC form, but if you have the required information, it should not be a problem. Enter the information they want to get, and submit the order. Also, some websites like TigerDirect will ask you for your DOB and will give you 3 verification questions to answer. Those are public records and can easily be found in your background report, so don't be scared. If you fail 1 question, you will be asked an additional question. If you fail 2 or more, the order will be put “on hold” and things will get harder, so try not to fail.

At this point, 2 things can happen when you submit the order. It depends on the spending habits of the cardholder, and will make things easier or harder for you.

1. The order goes through without any problem, and becomes “pending” status.
2. The transaction get declined and the website says to call the issuing bank. If this happens, call the bank, the system will act like the card is burnt (transfer without any additional questions), and a fraud agent will answer. Remember, the card is yours, tell them you authorized the transaction, but you don't know why it's declined. It's usually easy if you have the correct information, but if you ATO'd the account before, chances are that you have everything it takes.

When the agent tells you you are all set, resend the order on the website. Call as soon as you get the decline, don't wait, otherwise the real cardholder will get a call you don't want him to get.

All right, the order is now sent and the status is “pending”. The next section will tell you why some orders get canceled (newbie mistakes), and why in your case everything should be all right. Take a deep breath and hop to the next section.

Section 1.3 – Why Orders Get Canceled

When a website receives an order of about $1000, we understand that they try to protect themselves. What is the first thing that a website will do to verify the order? That's right, they will call the issuing bank and will check if the billing phone number you entered is correct, otherwise they will ask for it, and will ring it. You can receive the call, or the cardholder will, depending if you ATO'd the account correctly.

This is why orders get canceled when newbies enter a credit card order and expect to receive a free iPhone from the Apple store. They are not fools and want to protect themselves. However, if you took care of changing the billing number on file, you will get the call and you will be able to confirm the order.

Not so fast, a call is not simply “is everything okay?”, but rather a verification call where they want to see if you are really the cardholder or not. They sometimes ask you for verification questions similar toVerid questions, but all the questions are taken from public reports. They can also ask you if you put the shipping address on file with the bank (you hopefully did), and they will call the bank to verify.

Also, in some rare cases, they can make a conference call with you and the bank, but you will be asked for the usual questions, which means last 4 of SSN, DOB, last transactions, etc.

If you are a newbie and just put some credit card information on a website hoping to get a free iPhone, you will just see the order passing to Canceled state without any details and you will not even get a call. This is the reason why people post threads about “carding does not work” and get the same answers.

If you passed the verification call, the representative will tell you that everything is okay and that they will have the order shipped out today. This is good news! At this stage, I received 100% of my items, I never had problems past the verification stage. Now you may be tempted to hit another site; resist to the temptation. You ATO'd card can almost be considered a level 4 card, at you own the account and can do whatever you want, so it has a high sentimental value. Wait for the order to ship and the package to leave the merchant before you hit another webstore.

I recommend carding in the morning, to avoid letting a charge sit on the card for too long. You never know how often a cardholder checks his statement online. I had cards that died within hours, and other ones lasted 3 months. Once the package is shipped, you can card another store, no need to call the bank, as your drop address is already on file. Repeat until the card is burnt. Once it is burnt, never show your face at the drop again. The alternate address is on the bank's records and they can send Law Enforcement to this place. A drop is like a condom, use it once, do all your business, and trash it, because it becomes dirty.

Another verification step they can take is send you an e-mail asking for scans of your ID documents, such as passport and driver's license. These can easily be photoshopped and there are templates available everywhere. Utility bills are pretty easy to forge too, so don't worry about this part. Do what you have to do, but be quick.

Another step you can take, is to put the shipping name on the package to a family member of yours, for example if the cardholder's name is James Latyon, send the package to a certain Harry Layton (find a name that's on the report and have their DOB, in case) and say you are sending the package to your son / brother / whatever relationship you have on your report.

Also, keep in mind that no method is perfect, and the website can cancel the order simply because they feel it is not safe to process it. Nothing is perfect, but if you ATO'd the account successfully, it should be easy. Remember to stay under $2000 per order. You never know what other tricks they may use to catch you.

Always choose the fastest shipping method. Some say it raises flags, but if you did everything else correctly, that will not be the reason why your order fails. Besides, it greatly reduces your chances of getting an intercepted package, which is a pain in the ass and makes your efforts worthless.

This brings me to the topic of finding a drop to ship your order to. You can ship it to your house without any problem, if you want the police to knock at your door and make you ride dirty to the police station, and get in a steaming pile of shit of trouble. So read on to find out how to ship your order safely.Section 1.4 – Drops

A “drop” is a place, or location, where you have illegal, carded, or stolen goods shipped to. It has to be a place that has no link with your current life and is in no way linked to you.

Finding a drop is not really hard. You can go on Craigslist and find houses for rent, or just drive around your neighborhood looking for houses for sale where you can ship goods to. Make sure the house has no big windows that allow the driver to see that the house is empty. You don't want to have the package returned to the sender because of that. Just use your brain to find a decent house that you think is worth shipping a package to. Usually pick a town close to yours, but not in your neighborhood.

The big day has come: UPS tracking shows “Out for Delivery”. Yeah! Now check if the package requires a signature. All carriers require it, except UPS. For UPS, you can see if Signature Required is written on your tracking page.

Method 1: Acting like you are away

If you don't need a signature, you can leave a note on the door, “we are away, please leave package here, take this as my signature” and you might as well print the order confirmation page showing the tracking number and put it with your note to make your case stronger. The driver makes the final decision about leaving the package or not, but usually there is no problem with UPS when they don't need signature. Sign the note, put the order confirmation page with it, stick it in the door, and wait in your car not far from the place. When the driver leaves the place, grab the package, and put it in your car. Then skip method 2, and continue reading.

Method 2: Acting like you own the place

The second method is when a signature is required. You will have to meet face to face with the driver. Remember one thing, you can relax. The driver's job is not to investigate fraud, but only to make sure the package does to the right received. So you must just make him believe the package is yours, they don't care about fraud (but don't be stupid and talk about your crime). Carry a printout of the order confirmation page, the tracking number open on your smartphone (use VPN!), and look like you've been waiting for him. You might wait at the drop, sitting on the front lawn, or doing whatever you want. However keep in mind that waiting in the car when the driver sees you get out of the car is highly suspicious. If you choose to wait at the drop while being visible, take down any “for sale” or “for rent” signs, and call the bank's automated system prior to showing up to ensure the card is still valid and the police is not waiting for you. Greet the driver, show papers, sign the cardholder's name, and proceed to the next section.

By experience, when you have brokerage fees to pay (like international package), you can call UPS before getting the order and ask the amount. Leave a money order on the door and the driver will take it and leave the package. You will avoid getting a InfoNotice that way, and the driver will believe you own the place. I did that a lot of times and no failure so far.

After getting your package

I sometimes skip this part when I am lazy, but you should be extra careful. Your freedom has no price tag, so take 5 more minutes to do this precaution.Drive to a nearby park or public place, and open the cardboard packaging. Look for any device that may be tracking your position, such as bugs, GPS devices, etc. Then destroy the shipping label (you can burn it to make sure), throw the cardboard packaging away, and you now have in your hands a precious item you carded using your ATOd card. At this point, you can consider your carding heist a “success”! Drive home, relax, you owned the bank and the website. You can brag about it on the forums with reason.

If the card is still valid and there was no tracking device, you can card to the same drop again until the card burns. Get as much as you can out of it. Burn the card to a crisp. I remember getting $10,000 worth of electronics on a Chase card at the same drop, split on 5 orders. This was a money-making week.

All right, you carded the item, ATO'd the account, got items, more items, burnt that drop to a crisp too, now the card is dead... either over the credit limit, or flagged by the cardholder. Never show your face to that drop again, and enjoy your goods!

What happens after? Read on to find out.

Section 1.5 – Chargebacks

A recurring question on the forums is, when the card is declared stolen and the transaction is disputed because of fraud, who takes the hit?

In the case of a card-present transaction using chip & PIN in countries where they use that technology, the bank takes the hit when the transaction is declared fraudulent.

In all other cases, it's the unfortunate merchant that takes the entire loss. So if you card Newegg for $2000, they pay about $1600 for the merchandise that they send you, and they are short the money because you carded them, so they have to make 6 similar big orders without problems to cover that loss. You now undertand why they make verifications and don't want to be carded.

Some big merchants like TigerDirect and Newegg will just eat the loss and assume that they failed at fraud detection, but smaller merchants will make a formal complaint at their police department. Now, is the police going to investigate? It depends.

If a merchant reports a $200 loss for an order shipped out of state using a stolen credit card, there is a

99% chance that the police will not even open an investigation for that. However if they report a $3000 loss using a stolen card from the same state and shipped in a nearby city, LE (Law Enforcement) might move for that.

It also depends on the volume of complaints, the amount of loss compared to the size of the city, and whether there is an obvious pattern between fraud complaints or not. You should try to make your orders not linkable to each other, and use your common sense to avoid creating a pattern that might trigger an investigation.

It also depends if the cardholder himself decides to make a complaint or not. As long as they get refunded by their bank (which they do), chances are that they will not care and just forget all that. But some more mad people can decide to make a police report for identity theft. Again, there will be an investigation if there is an obvious pattern. It all depends which city you are talking about.So remember, when you card a website, they take the loss in case of a chargeback, so they want to protect themselves. You have to be smart and ask yourself, if I were in the shoes of the website owner, how would I catch fraudsters?

Section 1.6 – Warranty Fraud

A very fun type of virtual carding is warranty fraud. I got some $1000 CPUs from Intel and motherboards from ASUS using that trick. Here's how it works.

Many companies, especially electronics, offer what is called “advance RMA”. This is a type of warranty replacement where the company sends you the new product first, along with a return box for you to return the defective item to them. They sometimes ask for a credit card number in order to make sure you will return the defevtive item. This is where we can take advantage of the system.

It works will Dell, Intel and ASUS, perhaps a lot of other ones, but they are the ones I have experience with so far. You can PM sellers on eBay to ask for serial numbers of products, or you can simply card a product and request a RMA using its serial number. Call the manufacturer, say that your product is defective (use a diagnostic that makes sure it's really this product that is faulty, such as “the video card shows nothing on the screen, I tried 2 screens, but it works with other video cards”, and ask if they offer advance RMA, they mostly will. Use a level 2 card and have it shipped to your drop address. If they ask why, just tell them you are on vacation there and your computer broke.

When you receive it, take the package, and disappear. You just got more free stuff using a credit card that will eventually, maybe, get a chargeback, but you get the point.

For Intel, they ask for the 5 lines of text on the CPU itself, and a credit card for hold, so you need to have the unit in your hands for it to work.

For ASUS, the serial number is enough, they require a credit card.

For Dell, it's the easiest, no credit card needed, just order your free item on the phone without credit card, you just need a name and an address.

Feel free to discover weaknesses in other companies' systems, this is a relatively new kind of fraud and has not been patched. Many people use that to get free Xbox One from Microsoft. Most companies require that this warranty claim is done over the phone but don't worry, it's simple, and most of them don't seem to care about their job. I had 2 declines when carding Intel, the third one worked like a charm, and they did not even get cocky about it.

You can keep one for yourself and sell the other one on eBay or Craigslist, it's easy money to make.

The point is that they have to try to screen fraud at the same time than offering a seamless experience for legitimate customers. We just abuse the system.

Section 1.7 – Picking The Best Cards

If you don't have access to fulls, or you have a CCV autoshop and you want to get the best out of it, there's a trick that can save you money, if you have a bit of time to invest. It works with any autoshop as long as you can see the name and zip of the cardholder.First, search by desired BIN. If you like ATOs and you want good cards, BINs 426684 and 438854 work well, but that is up to you. If you can't search by BIN, just pick Credit Cards from any bank. Once you are in the list, find cardholders corresponding to your gender, and for each one, do the same thing.

Search their name and zip on Backstab or SSNFinder to check if you can find them. Most of time time (>50%), you will not, especially if the cardholder is under 45 years old. So just do the same for the next result. When you have the SSN and DOB of the cardholder, before buying the card, do this thing to double-check the info:

Go on peoplefinders.com and get their background report. Check if the DOBs match, and if the address list matches too, to make sure you have their SSN and DOB 100% accurate. When you are sure, buy the card, and buy SSN and DOB. You now have a fulls. You can go on archives.com or ancestry.org to get their MMN. Here's how to search;

Card an account on any of those 2 sites (level 2 card is enough, it's very easy). Get the mother's name on the background report, and search using her first and last name, and correct date of birth. Search for “marriage” records, if you can't find any, search “birth” records. If you don't find anything, try searching for the father's marriage records. Note that not every state / county has their records made public, so it's possible that you won't find it at all; it's okay, just make one up when you ATO the card.

This way, you can scrub the autoshops and select only the cards where you can have full information. This is my trick to get only good cards. Of course, the best option is to find a fulls vendor, but there are not a lof of them, so escalate your cards the way you desire.

Then, just check the balance, study the background report, and you are ready to hit big shops and get stuff at your drop!

Section 1.8 – Commercial Fraud

Want another (and probably easier) to get items shipped to your drop and getting tired of carding Newegg and TigerDirect? All right, I'll show you another method for that. This method works best for Canada but is really good for USA too.

You can find any major provider that only sells to commercial customers. For computer parts, for example, you can targer ASI, Synnex, and so on. The goal is to get the business registration certificate of a business in the town you wish to have your drop. This certificate is usually public data and can be found on the registration records depending which state or province you are in. Once you got the business registration documents from a business that operates in the same field of activity you wish to get items for, you are ready to hit the provider.

Apply for an account at one of those providers using that document, put all the business address info, but put a drop address close to that place, and your burner phone number. Both providers (ASI and Synnex) usually don't call, but just in case, better stay safe. It usually takes 24-48 hours to open an account. “Your name” is the name of the real business owner. On the credit application, do not request net terms, just write “no credit” and let them know you will pay before getting items shipped.

On the credit card authorization form, put the cardholder's (pizza) name, address, card number, expiration date, CVC code. Let them know that this person is an “officer” at your business, such as aremote sales representative. Once the application is approved, you are good to go and hit big amounts.

The reason is that they do not make verification when sending orders, as they almost never get fraudulent orders. They assume that commercial customers are always going to be legit, but in fact, we use someone else's business documents to trick them into thinking you are the business owner.

I was able to pull over $5,000 per order using that technique; the merchant is considered low-risk so there are very few declines, and verifications are almost nonexistent. With computer parts, it's extremely easy to do that, you can try other commercial providers. Now you are playing in the big game, and the possibilities are endless. Make sure to never show your face at the drop once the card burns, as they will really try to find what happened.

Section 1.9 – Newegg And TigerDirect

Always wanted to card those 2 big merchants to get electronics? I will tell you how. This is normal difficulty if you know what you are doing and if you are good at social engineering. You need, at the very least:

1)
2)
3)
4)
5)

Cardholder's account ATO and billing phone number changed to your burner
Shipping address on file with the bank
Full background report on the cardholder
Story about why you ship to that address
Local area of the cardholder: restaurants, shopping malls...

And remember, mail forwarding companies are blacklisted by those merchants. Don't try shipping to MyUS, Bongo, and so on, as it will automatically cancel the order. Which American would use a US card to ship to a forwarding company to get it out of the country? None. Have a normal drop address.

Number 5 might seem strange, but it's true. Some people, including myself, have been asked “can you name a local restaurant near your house” to make sure you are the cardholder. So it's not a bad idea to get familiar with the surroundings (major malls and restaurants) in case that happens. You'll thank yourself later.

So, take your time to browse, look around, read descriptions, and appear like a legitimate shopper. Once you did that a few days and the account is ready, send the order, and try not to go over $2,000. The order will be placed on “hold” status, and you will have to talk to the verification department. I will describe the procedure for TigerDirect, but Newegg is fairly similar.

TigerDirect's website will ask you for addresses, credit card information, then you will have to pass VBV/MCSC. After that, they will ask you for your date of birth. Then, 3 verification questions will pop. They are public record information about the cardholder and can be found in your background report. Try to have so much information that you feel like the cardholder is your friend. Answer the 3 questions and be quick. If you fail one, you will be asked an additional question. If you fail 2 or more, forget your order. Once you send everything, your order will be “on hold” status. You need to call the verification department. Conversation goes as follow, usually:

Rep: Thank you for calling TigerDirect verification department, can I have your order number?
You: 123456

Rep: All right, what is your name?

You: James LaytonRep: Thank you Mr. Latyon, let me verify the order for you.

(you will be on hold about 2 minutes)

Rep: Thank you for holding, is <name on the package> a tenant at the shipping address?

You: Yes (giving the wrong answer voids the order)

Rep: I could not locate that person in the system. So you will be offered 2 options. Either we ship to your billing address, or you need to call your bank to add the shipping address as an alternate address on file so we can ship there.

You: I already did.

Rep: Oh really? All right then, let me verify that for you. Please wait.

(you will be on hold while they call your bank, sometimes they can make a 3-way call)

Rep: All right, I see the shipping address is on file. Thank you, and is it okay if I call you on that phone number, 123-456-7890? (whatever phone is the primary billing number)

You: Yes, sure.

Rep: Thank you, hold on.

(the phone will ring, pick the call, or the order will be void)

Rep: All right, we have successfully verified your identity Mr. Latyon. We will have the order shipped out to you tonight.

See the pitfalls in the dialog above. You must assume that the shipping name is a tenant at the address.

For example, if the cardholder's name is James Latyon, you can ship to a Joseph Layton and assume it's your son, but make sure that name is on the background report and you have their DOB. Sometimes they may ask for it if they get suspicious.

Next, you must make sure you can pick the phone when they call the “billing” number. If you do all that correctly, you are good to go and you will get your parts. They do not ask for scans of documents, everything is done over the phone.

Section 1.10 – Stripe Cashout

If you're not really into carding physical products, then you might want to be interested in how to make actual money with your cards. For this technique to work, you will require:

1) A bunch of level 2 cards (address is not required)
2) HTTrack program (can be downloaded for free)
3) Notepad++ program (can be downloaded for free)
4) Drop bank account
5) Dead full (name, address, DOB, SSN), referred to as “cardholder”
6) Basic computer skills

The first step is checking on stripe.com to see if your country is in the active list. If not, you might want to get a bank drop in an active country, usually USA is the easiest.

The first step is creating a fake online e-shop. This is very easy, you can google, for example, “usa clothes online”, and jump to page 12 of the results, to get smaller shops. Try to find a shop that has a very simple design, about 100-200 items, avoid big ones. Take one that do not seem to use Javascript a lot. You will maybe have to look 4 or 5 shops to find that one.

Then, open HTTrack, start a new project, and mirror that website. This will create a local copy of that website on your computer. In the best case, try to stay under 800 – 900 MB. Once you have a local copy of the shop, check if you are able to browse it, view items, etc. Of course, the whole shop won'tbe functional, for example, you will not be able to register, that's normal. Try looking item descriptions, browse categories, and look like a normal user. Once this is done, you now have a copy of that online shop, already pre-made, and it took a few minutes (maybe hours) to mirror, but you don't have to stay in front of your computer.

The next step is to open the contact page using Notepad++ and editing the contact information to a custom name you decided to make, and the address / phone number to match the cardholder's address and phone. If there's a Google Map, make sure you edit it too. This is where the basic computer skills come in handy. If you have absolutely no idea how to edit HTML, I suggest you get an online course, as this can be an invaluable skill. It's very easy to learn.

Look for some footers, privacy policies, and terms of use where the old name may appear, and edit it. Use common ense here. You now have your custom clothes shop, that took less that 1 hour to make, and you appear to have a legitimate business. Yay!

The next step is hosting your website. It is important that you use an anonymous host, so for this example, we will use bitcoinwebhosting.net. I used to have this one a lot with my fraud sites. Use a made-up Hotmail address that corresponds to your cardholder, open an account on your hosting company, and host your files on it. Almost all hosts will allow you to register a domain. They might ask for address info, so just give them your cardholder's address info. So setup the account, register the domain, and host your files for the fake shop. Just upload them via FTP (if you don't know how to do that, get basic lessons). Make sure your shop is online and works, for example, let's assume your shop is myfraudsite.com. Make sure that myfraudsite.com displays your shop and that you can browse.

Then create an e-mail address related to this host, usually with the prefix “admin”. In this example, we will create “admin@myfraudsite.com”. This makes you look legitimate. At this point, you should have your online “shop” working, and an e-mail address associated with it. Everything should be hosted on an anonymous host. They usually charge $10 per month in bitcoins. We are now ready to start making money with our fraud site.

Open an account on stripe.com using this e-mail address and keep the account in “test” mode. Create a page named “charge.php” and upload it to your web shop. This will be the file you use when you send a charge. Here is the code you should put in the page. Note that you can adapt the code as you wish, but that's my personal example:

```
<?php
require_once('./lib/Stripe.php');
Stripe::setApiKey("sk_live_xxxxxx"); //<- This is your Stripe key
try{
echo "Processing...";
Stripe_Charge::create(array(
"amount" => $_GET["amount"],
"currency" => "usd",
"card" => array(
"number" => $_GET["number"],
"exp_month" => $_GET["month"],
"exp_year" => $_GET["year"],
"cvc" => $_GET["code"]
),
"description" => "This will appear on the card statement"
));echo "Charge OK"; //Success!
}
catch (Exception $e){
$error = $e->getMessage();
echo "Error: ".$error; //Failure.
}
?>
```

Take time to understand what this code does. You will call this page using this query:

```
http://myfraudsite.com/charge.php?
number=4266841200000000&month=2&year=2016&code=333&amount=6800
```

This will charge an amount of $68.00 to the card 4266 8412 0000 0000 expiring February 2016 with CVV code 333. It's simple like that. Change the parameters to plug whatever cards you have, and try to vary the charge amount too.

Make many variations using the test key to appear like you really made some testing. Make charges and see the result, and get familiar with this code snippet.

When you have a working example, switch your Stripe account to Live mode. You will be asked to provide the name, address, DOB and last 4 of SSN of your cardholder, so just proceed. Ignore the tax number part, put the website address, put a small description of your choice, and put the account in live mode.

Now you will be asked for your bank information. This is where you will provide the routing number and account number of the bank drop where you want to receive the money. All information is filled and you are ready to make money!

You can use any autoshop to get a lot of cards. You only need the card number, expiration date, and CVV code to proceed. Get cheap cards, this is the easiest transactions you will have to do. You can try Vault Market, which provides $4 USA cards at the time of writing. Beware though, you have precautions to take to avoid getting your operation shutdown, so read the next part before you go crazy with the cards.

First, you must keep an approval rate over 50% on all your transactions. This means that over half of your transactions must be approved. So you should have a good card source. If the decline rate is too high, they will refund all payments to the cards and close your account.

Second, you must use cards from the same country your fake shop is supposedly based in. If you have a UK shop, use UK cards, even if they are more expensive. Not 100% of your cards must follow this rule, but try to keep it over 90% to avoid suspicion.

Third, vary the amount of the charges you make. Vary a lot, for example, between $50 and $300 per transaction. Do not go over $300 as you might get declines that count in your 50% approval quota. You don't want to get shut down. Also, try to wait a bit between transactions, even if you love money. We all love money but keep it looking real.

The rest should be common sense. The money gets deposited after 7 days for the first transaction, and 2 days for subsequent transactions. There is another approach which has been tested once and proved tobe successful: the anon card. We can be afraid of chargebacks (I'll talk about them later) coming in before 7 days, so here's how we can bypass it. When your account is in live mode and running, use an anon card to make a transaction of around $100 (you get the money back in your bank drop anyway), and 3 days later, use another card to make a transaction of $50. The money will obviously not get charged back and will be deposited in 7 days. When this is done, start hitting with real pizzas. This way, you get rid of the 7-day barrier that might get you closed.

Now, what about chargebacks? If a customer disputes a charge, mostly with “Fraudulent” code, you will get an e-mail saying that the charge has been disputed, a $15 chargeback fee to pay, and the amount will be deducted from your next transfer. This is up to you if you feel that the number of chargebacks is acceptable against the number of cards you can process. Make your calculations, and when too many chargeabacks start kicking in, time to trash it.

To trash an account, just close your drop bank account, or charge your account info in Stripe to another random account (same routing number). Delete all files from your hosting, put the files of a new fake shop, register a new domain, open a new Stripe account, and start over.

Repeat until your wallet is full. Always use VPN when accessing your website or Stripe, you don't want to leave your real IP for LE to get back to you and knock on your door!

I made several thousands of dollars using this method and it cannot really burn. Up to you to discover what works best for you!

Section 1.11 – Beyond the ATO – The PTO

When you commit Account Take-Over fraud, also known as ATO, you take “ownership” of the victim's account. Even if you change the phone number on file, they still keep record of the previous phone number. This is where this section will prove useful. I will give you the transcript of a failed ATO I had 2 months ago, and you will understand.

(pass verification questions)

Me: I am calling because I tried to place an order online, but it got declined. The charge is $1500 and the merchant is Newegg.

Agent: No problem Mr. Johnson, let me see what I can do for you, can you please hold?

(by experience, if they put you on hold, hang up, it's most likely burnt, here it took 5 minutes)

Agent: Hello?

Me: Yes madam, I'm still holding.

Agent: Unfortunately I will not be able to let the charge go though, and I can no longer provide service on this account.

Me: How about my card? What should I do?

Agent: You can destroy the card, as you are not the real Robert Johnson.

This is a situation that sucks, and there's a way to avoid that. It has to be done before calling the bank.

What happened here is that the agent called the previous number, even if I changed it a few days ago. The real cardholder got the call, and you can imagine the rest.

First of all, take the real phone number of the cardholder, and use WhitePages to find who is the phone provider. If you cannot find it, then you might want to use Spooftel and call the various providers (AT&T, Verizon, Sprint, etc.) and use their automated system to try to find out if the number isregistered with them. You can use phonevalidator.com to see if the phone is a cellphone or a landline.

When you have the background report of the victim, you can see that they often have many phone numbers. Use the service to find which one is landline and which one is cellphone. For cellphones, it's very easy to find the provider, as most of them allow you to call the phone and press * (star) to go in the voicemail settings, so you recognize the greeting. Use your logic, and write the phone numbers, probably like that:

Phone 1, landline, 555-123-4567, Verizon

Phone 2, cellphone, 666-234-5678, AT&T

Now, remember, you have the full address, DOB, SSN, and more information on the cardholder, and you know what is his phone company. What are we gonna do? That's right, Call Forwarding!

Call up the phone company using the opposite phone (if billing number is the landline, call with the cellphone, and vice versa), spoof the number. When you talk with the customer service department, it might go as follow. Don't forget that it's less secure than banks, as it's not about finances. But it can have worse consequences.

Agent: Thank you for calling Verizon, my name is Mohammed, how can I help you?

Me: Hi! I will be away from my house in the next days but I'm waiting for an important call on my landline. Since I cannot reach the other party, I would like to set call forwarding so I will receive the call on my cellphone.

Agent: No problem, can I have your name?

Me: Barack Obama.

Agent: Thank you Mr. Obama, what is your full address?

Me: 123 fake Street, Washington DC, 12345.

Agent: Thank you, and may I have your date of birth?

Me: October 1 st , 1845.

Agent: Thank you. Did you know that you can press *72 on your phone to activate call forwarding? This is an easy way to do it without calling customer service.

Me: Thanks for the tip, however I'm not home at the moment, so I am unable to do that.

Agent: Okay no problem, I will activate it for you. What is the phone number you would like the calls forwarded to?

Me: That's my cellphone, 456-123-3245. (your burner phone)

Agent: All right, and you want it to start now?

Me: Yes, please.

Agent: No problem, I activated it for you. When you will be home, you can use *72 again to deactivate the forwarding.

Me: Thanks.

Agent: Is there anything else I can help you with?

Me: Nope, thanks.

Some phone companies, AT&T by experience, ask for a 4-digit PIN, but it can be easily bypassed using DOB and last 4 of SSN. The good point is that, if you are extremely unlucky and fail (which should not happen because it's easier than banks), the card will not burn. This is the PTO, Phone Take-Over fraud. This word was invented by me.

Now you are ready to call the bank to ATO. If they decide to call the billing number (happens very rarely), you will answer the phone, and it will destroy all suspicions they have. The cardholder willprobably be locked out of his account, but that's not your problem. The first dialog (failed ATO) can be avoided if you do that before.

When your business is finished, do not forget to call Verizon (or his company) to deactivate call forwarding. The goal is to get free stuff, not make the cardholder lose friends because they can't reach him, use a bit of compassion. If you think you will need his phone line for a few days, you can use RingCentral phone system and decide which numbers you want to take the calls from, and which ones you just want blindly transferred to the cardholder. He will probably never notice that someone fucked with his phone line, but will notice the charged on his card!

Some websites do not require the shipping address to be on file with the company; in those cases, you can do a PTO without doing an ATO, and put the correct billing number on the website. Take the call from them and confirm the order, and restore his phone line. Use your imagination for the rest.Chapter 2 – Protecting Yourself

This chapter is all about protecting yourself when carding online. When getting free items is fun, the police side of the operation is less fun. You will learn techniques to make sure you are untraceable when commiting online fraud.

Section 2.1 – Protecting Yourself Online

We are going to discuss about how you can protect yourself online when making fraudulent orders. We will talk about your 3 best friends: VM, VPN, SOCKS.

Friend 1: The VM

The VM (Virtual Machine) is an installation of Oracle VirtualBox or VMWare, whatever you prefer. It's like a computer in your computer. Your computer is the “host machine” and your VM is the “guest machine”. In your guest machine, put everything related to carding. Never put anything fraud-related outside this VM. Keep everything at the same place, you don't want to leave proofs on your computer.

Once your VM is all-set, create a TrueCrypt volume and put your VM files on it. Only mount your TrueCrypt volume when you want to access your carding stuff.

By using TrueCrypt, you ensure that your VM is all encrypted, and that everything related to carding “vanishes” when the power is switched off, and you need to decrypt the volume again to access it. So if LE barges in your house, pull the plug on your computer, and all proofs are gone. No need to start deleting files here and there. If they seize your computer for analysis, there will be nothing to find. Your VM is totally invisible and only accessed when you want to card something.

Now that your physical computer is protected, you will need to think about hiding your identity online. If you do not know much about VirtualBox and TrueCrypt, you should to research on them, they have many uses outside of the carding world too.

Friend 2: The VPN

The VPN is the way you can use to hide your identity online and appear anonymous. It routes all traffic from your computer to a VPN server that hides your identity and forwards the traffic to the desired site.

I personally use PureVPN but you are free to take any provider, but read their privacy policy to make sure they don't keep logs.

If you fail to use a VPN, your IP address will be visible. The police has only to call your ISP and get your information from your IP, and you are busted. So using a VPN is crucial for anything sensitive online. Once you think your VPN is correctly connected, you can type “what is my ip” on Google to find your location. Make sure the location is the advertised location of the VPN server, and not your real location.

With the VPN, you are anonymous, so everything you do is hidden. Only problem, merchants know that too. Although they can't know who you are when you browse their site, they can see you are using an anonymizing service and therefore it's more likely that this order will be fraudulent. It raises flags.

Many major merchants have a list of the known VPN servers and flag the orders originating from those addresses. So our next friend will solve that problem.Friend 3: The SOCKS

We are not talking about underwear here, but about a Socks 5 proxy. What is that? Simple. In order to make sure you look legitimate to the merchant, you need to become the cardholder. If you go on vip72.org, you can buy socks from many cities in the world. If you choose a socks in the city of the cardholder, you can appear like you are from that city when you make the purchase and therefore have higher chance of success.

When you install the VIP72 software, you will be able to choose among a variety of socks by city and those are not blacklisted as they are not public anonymizing services. It's like using someone else's computer (in that city) to make the purchase. This way you genuinely appear to be the cardholder and you eliminate all the problems.

Use SOCKS over your VPN for maximum security (in case the socks proxy is compromized) and you will not be traceable. By combining that with your encrypted VM, you ensure yourself a rock-solid setup with no possibility of being traced. Once you pick your item at the drop and leave, it's gone forever, no way to get back to you. Success!

I see a question that comes often on the forums, how do we chain socks and Tor? Simple. First, don't use Tor. Use any browser like Google Chrome. Here's how we use the full setup.

1) Get a VPN (like PureVPN) from USA (Vip72 likes to hang when you use a non-US VPN location, so don't take any chance).
2) Connect the VPN, open VIP72 program.
3) Log in, select country, state, city, then double-click your desired proxy.
4) When the proxy is in the selected list, open Proxifier.
5) In your browser's proxy settings, select “use system settings”.
6) Google “what is my IP” and make sure you appear in the desired city.

If “what is my ip” shows the desired city, and your VPN is connected, you are invisible now and you can card whatever your heart desires. Don't skip the VPN, you never know when/if the socks will rat your location. Better be safe than sorry.

Another way LE can catch you is by your username. On TCF and on Evolution Market, some LE officers have accounts, and are looking for “big shots” to catch. A step that LE takes is to Google your username and find clearweb sites that you might be registered on, in order to have a starting path for their investigation, so use a username different from your clearnet operations.

They will check who lives at your drop and make a list of family or friends, so make sure you are not linked to that place in any way (business, friends, family, etc.)

They can use voice recognition to catch your voice on a call. This is not the way to get you caught, but it will serve as an additional proof if you ever get convicted of that crime.

Section 2.2 – Burner Phones

This section is about how to call banks safely, and avoid being traceable. If you use your home phone for that, you will get busted for sure. Here's how to solve that problem.The first step is registering a RingCentral account (you can card it with a level 2 card) where you will be buying the phone numbers required to impersonate all your cardholders. Go on ringcentral.com and register an account. They will then ask you for a phone number where they can reach you. You can make an excuse like you are at work and you will call them when you have 2 seconds. Call them and talk with them, and agree to a office plan. You can say you are going on a vacation for a few months and you need a IP phone to call home for free. This process is fairly easy.

Once you have the RingCentral account set-up, take some time to explore the options in their interface, learn how to register phone numbers. You can select by state and city to register phone numbers and point them to your burner face. They often change their interface so I will not go in the details here, but make sure all “burner” numbers will ring your burner cellphone. As an alternative to that, you can get a desk phone, configure the SIP information in it, configure port forwarding in your router, and, if your router supports it, select VPN at the WAN connection type, so you have a protected desk phone that can be on 24/7. A burner cellphone works, but since there is no VPN possibility for calls, can be a bit of danger. You can always get prepaid SIM cards under a fake name for your cellphone, but since the IMEI of the phone can get flagged, we recommend getting a cheap $10 phone and throwing it away after each big heist.

If you choose the desk phone, no need to throw anything away, as the location can never be traced by any mean if your router uses a VPN connection. This is the option I personally use. Just make sure you are available to take the confirmation call from the merchant, as a missed confirmation call is often synonym of failure. They are paranoid like that sometimes.

Many Polycom, Aastra or Cisco phones do the trick for burner desk phones, as they also have legitimate uses. You can also have a legitimate line and a fraud line if your phone supports 2 SIP lines, which most models do. Everytime a card burns, I change the card on RingCentral, and I have yet to see a terminated account because of chargebacks. So far so good, and it's been months. When spoofing the cardholder's number, there are 2 very popular services, Spooftel and Spoofcard.

Spooftel accepts only bitcoins for payment, but they are pretty cheap, only $0.10 per minute to any number and they don't block numbers for nothing.

Spoofcard accepts credit cards for payment (you can card them with a level 2 card) but often, the calls cut after 30 seconds for no reason, for all kinds of reason, so I stay away from them and I use Spooftel even if I have to fork over some bitcoins.

Be careful, as LE can subpoena any of those 2 companies to reveal the number you used to make the spoofed call, so don't use your real phone to make the conversation, as there is a way to trace it to you.

Use your burner combined with Spooftel for maximum security.

Section 2.3 – AVS

AVS is Address Verification System, a fraud prevention system used by shops to make sure the billing address is correct.

It works by computing the numeric part of the address (street address and zip code) against what's on file with the bank to make sure it is accurate. It compares only the numeric portion only; so 123 Right

Street is the same than 123 Wrong Way. The zip code is compared in full.Why is AVS important? Because it causes automatic declines on many site if the AVS does not fully match. If the cardholder can't write his own address, the website will not believe for a second that you are the genuine cardholder. Many sellers sell non-avs cards. Is this good? We'll see.

Let's say you have a non-avs Amex card from Colombia (those are very popular). People tend to use those on USA online stores and put the billing address and shipping address to be the same, hoping the card will pass AVS. It will. But...

A clever fraud screening agent will see that the BIN is from Colombia. What is the chance that someone with a Colombia card has a USA billing address on file, especially knowing the card is non-avs? That's right, very slim. Expect the order to be cancelled right away unless the fraud agent is very stupid (they are getting more and more clever those days).

Non-avs card are to be taken with caution. Do not assume you are able to card any shop with these just because they do not use address verification systems.

Section 2.4 – Flight Tickets

Another popular question is, “how do I card flight tickets?” although this is doable, I advise against it because it's dangerous. If you still want to do it, I'll tell you how.

If you are carding a local flight, usually there is no danger. You should use a card from the same country than the country you are flying in. You can put your real name, or put the cardholder's name and use a fake ID. If you choose to use your own name, make sure you have evidence supporting your case if you get pulled over while boarding or getting out of the place. You can say you purchased tickets from Craigslist or a forum, but have some (fake?) evidence supporting it. You want to avoid all credit card fraud suspicion in case problems happens. Better be safe than sorry, although I've done that many times and I never had problems. If you use your real name, use any ID except your passport, this can save your ass later. Use a non-government ID such as student card, in many cases they accept them. Present a government ID if asked to, but no passport.

If you are carding an international flight, that's harder. You have to use your real name and passport number. Be aware that it does not make you a fraud suspect in case of chargeback, as they can't prove you carded it yourself, as long as you took your precautions on the computer. Show at the check-in and go to self check-in to avoid people as much as possible. Try to card a short flight, and avoid first class flights (it raises flags). Upon arrival, get out of the airport as fast as possible. If you didn't get caught, good job! Otherwise, well, nothing because you don't have this guide in jail.

In all cases, you should never card the airline directly. They have representatives waiting at the airplane exit just to catch fraudsters. Card third-party websites like Expedia, Cheapoair, etc. as they can't move fast enough to catch a carder. If you card them successfully, you have thin chances of getting caught at the airplane exit.

Now, this has been discussed before, but do not card hotels! You do not want security staff to knock at your door at 3 AM to talk about fraud. If you go on a trip, card a part of it, but I assume you have a bit of money too if you go on a trip. Use common sense.

Card only one-way flights, do not card return flights unless they are very close to each other (2-3 days maximum). If there is a chargeback and you are waiting for your return flight, be assured they will waitfor you.

Last but not least, have strong arguments if you get intercepted at the exit. Like you purchased it from someone else. Leave no proofs of any carding evidence. This is common sense but it's alwayss welcome to remind our fellow carders.

Section 2.5 – Glossary

This is a list of common words used in the carding world, and many people are not sure of their meaning. Here are some of them.

ATO: Account Take-Over. This is when you call the bank while impersonating the cardholder to perform whatever operation you want on the account.

CC: Credit Card. You know what this is.

CH: CardHolder. The real owner of the card.

COB: Change Of Billing. This is changing the billing address when doing an ATO. Be careful as this may trigger a ring to the cardholder.

CVC: Card Verification Code. Also known as CVV or CVC2, this is the 3-digit code behind the card near the signature panel (4 digits for Amex cards).

DL: Driver's License. Used for verification purposes.

DOB: Date Of Birth. You know what this is too.

MCSC: MasterCard Secure Code. Also known as MSC, this is the security mechanism that asks for verification questions during an online purchase made with MasterCard.

RC: RingCentral. Your favorite source for burner phones.

SSN: Social Security Number. You know what this is.
VBV: Verified By Visa. Same thing than MCSC but for Visa cards.