Carder Science

Fourth Edition

September 1st, 2014

Written by alpha02

Carder Science, Fourth Edition

Written by Alpha02, Moderator @ TCF, September 1st, 2014

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
- 1.12 - Maxmind Fraud Prevention Algorithm
- 1.13 - Order Verification Procedures
- 1.14 - Stripe Automated Cashout
- 1.15 - CC to BTC
- 1.16 - Squareup Cashout
- 1.17 - Flint Cashout
- 1.18 - PayAnywhere Cashout
- 1.19 - Getting Asked For Photo ID

Chapter 2 – Protecting yourself
- 2.1 - Protecting Yourself Online
- 2.2 – Burner Phones
- 2.3 - Spoofing Android Device – The Perfect Way
- 2.4 - AVS
- 2.5 - Flight Tickets
- 2.6 - Spoofing E-mails
- 2.7 - Completely Spoofing Your Identity
- 2.8 - Safeguarding Your VPN
- 2.9 - The 10 Most Common Mistakes
- 2.10 - Glossary

Conclusion

Introduction

This guide was written by Alpha02, Moderator 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, only a few select VIP members 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.

Why am I not letting this information go for free? Simple. If we post good and working methods in the open, all newbies will try to exploit them in any good and bad way possible, burning it before the pros can start making money with it. So by asking people to pay for a complete guide, we ensure that those methods will not burn in the long run. We strive to provide quality information!

This guide was written with the intention of helping people who are ready to invest some money to make money. We can't let newbies registering and seeing top-secret methods in the newbie section of the forums, as it would destroy everything.

The Stripe cashout method is the most popular one and is the one people make the most money with because of its easiness when explained in that guide. On June 2nd, 2014, I made enough money with Stripe to buy a brand new Mercedes-Benz with a suitcase full of money. Everything is possible, and since your purchased that guide, you now have access to the elite carding methods.

I've always dreamt of becoming a millionaire in the real estate field. Everybody knows, to be able to afford real estate, you need money to put as a cash-down payment. Tons of money. And I don't believe in working 40 hours per week to bring home a mere $400 per week, minus all the bills, and count how many pennies are left in my pockets. I believe in living rather than surviving.

And even with a real-life business, that's still not enough. This is where I discovered the world of online fraud. I lost a bit of money in my early times beleiving that dumps + PIN actually existed, and Mr. Fungi probably laughed at several people that way. Carding helped me, as a few other people, pile up money and afford what we always wanted.

Carding is not all; a very lucrative field is payment processor cashout. I will detail 3 techniques commonly used by fraudsters to increase their illegal income. Most importantly, when your things start to go well and you see the money, do not brag to anybody! You never know when a friend will threathen you to rat you out if you don't do a favor. I'm a legit-looking man, never smoked of my entire life, only here to get some money.

After reading this guide, you will have the knowledge to card virtually anything. You can get free computers, electronics, clothes, and much more. Since this knowledge can be very dangerous, I encourage people to stay ethical in their doings. For example, avoid carding your local mom & pop store, since they can barely eat losses. Go for the big fish, the ones who deserve it, like Walmart and Newegg. They are cardable. If you failed many times at carding them, you have the right book.

There is no website considered “uncardable”. Everything can be carded with the right level of attack (first chapter will talk about site attack levels from 1 to 4). I personaly carded every site that people

thought were uncardable. Some were really hard, but if you “become” the cardholder, you will be able to do miracles with fraud. At this date, not all online merchants are aware of credit card fraud. Some will simply process every transaction that comes their way, while others have advanced fraud prevention. This just gives us an extra challenge.

Some methods were found on the forum, then perfectioned and adapted to make it viable and cardable. Most of the time, it is a game of cat and mouse, but there's a point where stores can't step up more security without seriously compromising customer experience. We must take advantage of that, and look like that customer who is confused about how he uses his card.

Life is short; if you have dreams, get the money to realize them! The cashout methods in this book are here for this purpose and will give you a nice starting kick to get the financing for your projects. As for the question “is it possible to life a life out of carding?”, the answer is yes, but I don't encourage it. I recommend using carding and cashout to get money for legit projects, something that you can show to society to make people proud of you. This is how you get people's respect, and this is how you get all the girls.

Enough talking, let's get started!

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 sites 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 1st, 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 1st, 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.

There is also a technique that works well with Citibank: when you are asked for the MMN by the automated system, if you fail, you will hear “the agent might need to ask you verification questions”, and if you succeed, you will be connected and everything will be a breeze. When the automated system asks you for the password, say “Jope” while putting a high tone on the O sound, then slightly lower your pitch. Say the word at normal speed, like when you are talking to someone. This will trick the automated system into beleiving that you got it right. You might have to retry 2-3 times for it to work, but I got it with almost all my accounts. This will save you a lot of hassle with the agent and will make the call extremely easy.

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. All US banks accept a Canadian address, and some banks may accept an international address.

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 to Verid 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. If nothing mentions a signature, or if you are not sure, then signature is not required.

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.

Sometimes, the driver might get cocky and ask, why your name is not the same one than what's written on the package, or why you're not inside. You can tell that you recently moved, and you put it under someone else's name because you have “problems with customs”. When they get cocky, you can threat them to make a complaint at their local UPS hub, they usually calm down and hand over the package. I had a cocky driver in my last carding trip in Minnesota, and I had to use this method, and I finally got my package.

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.

Picking your package at the UPS facility

In some unfortunate circumstances, the package can end up at the local UPS facility and will require government-issued ID to be picked up. This happens if you missed your drop, for example. In that case, don't bother making a fake ID, as there is a better trick.

The package is usually held for 5 business days before it is sent back to the sender. The day the package arrives at the facility is day 0. Two scenarios can happen:

Scenario 1: You get a call from the UPS branch

They will probably call you and say something along the lines of, we have a package for James Fakename waiting at the facility for pickup. Just tell them that you don't know this person. Here's a sample script of what it should look like:

UPS: Hello, may I talk to James Fakename please?
You: I think you may have the wrong number, who is speaking?
UPS: This is the UPS branch, we called the phone number we had on the package.
You: Oh, I was waiting for a package too, and it didn't get delivered. Is this a package from Newegg, a smal box?
UPS: Yes, we have one small box waiting here, for James Fakename.
You: I have a tracking number, can you check if the last 4 digits are 3382?
UPS: Yes they are.
You: I'm very surprised, because my name is Fake Name and I was waiting for this one. I have no idea who James Fakename is. They looked confused when I placed the order too.
UPS: Well, the package will be sitting here, just come pick it up when you are ready.

This worked me twice. I had 2 drops to watch at the same time and I missed one package. This allowed me to pick it up.

Scenario 2: You do not get a call

On the morning of day 5, call the toll-free number and ask to be transferred to the local branch. You can do the same scenario, and inquire about a package waiting there for you. You must look confused a bit in your voice and look like someone who was victim of a mistake from the online store, and they will gladly hand over the package to you. Everytime I did it, I never got asked for any form id ID and it was

all smooth.

Do not give your real name. Test the card before going (call the bank), and only do it if the card is still live, otherwise it can be dangerous. You can also send a mule if you are too afraid, but I showed my face a few times when the card was still live and never ran into issues.

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. Also burn the order confirmation page if you decided to go this route and you brought it to the drop! 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?

Sometimes, you might receive an e-mail from the store asking you to provide more information about the chargeback, such as authorization forms or documents. Just ignore that e-mail. Do not become cocky and answer “I got you!” because it could be the difference between an investigation or not. Keep it dead.

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.

Make sure your cards are well organized. I have included a sample Excel file where you can see how my cards are organized. All cards can be sorted by name, address, number, expiration, DOB, SSN, etc. Look at the file for more information. Also, use line colors for different meanings. Example, white rows mean that the card is mine, and still not used. Call the bank before adding the card to the list, because you want to trash junk cards right away. Yellow means that the card is burnt, and blue means

that the card is currently being striked, so I know what to focus on. Green means that I fucked up the cardholder's credit history using his DOB and SSN. When you look for fulls, look at your Excel file, and with the colors, you can find your card quickly.

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 a remote 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) Cardholder's account ATO and billing phone number changed to your burner
2) Shipping address on file with the bank
3) Full background report on the cardholder
4) Story about why you ship to that address

5) 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 Layton
Rep: 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.

It is also a good practice to avoid Hotmail addresses; anyone can make a fake Hotmail under someone else's name. You should use a custom e-mail with a custom domain. If you read the next part (section 1.10 – Stripe Cashout), you will see how to setup your own domain. Let's say your fake shop is bestclothes.com, and your cardholder is named James Layton, you can create an e-mail jlayton@bestclothes.com and it will look like a commercial e-mail address and will lower the red flags. Trust me, it plays a lot when carding hard merchants.

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't be 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!

Use Notepad++ to do a search & replace for the regular expression “<!-- Mirrored[^>]*GMT -->” (never include the quotes in any example) and replace it by nothing. This will remove all the “Mirorred by HTTrack” comments in the source code, in case they look at it.

However, you might get a bunch of folders in your website directory. Let's say the mirroring is finished and you have a www.fakeshop.com and a img.fakeshop.com folder. You want to move the img.fakeshop.com folder and put it inside the www.fakeshop.com folder. Then do a search & replace for “.../img.fakeshop.com” and replace it by “img.fakeshop.com” in all *.html files, and everything will be good. Repeat for each concurrent folder you have. Make sure you can open the index.html page in your www.fakeshop.com folder and everything shows up correctly.

Do a search & replace for the phone number of the shop and replace it by a random toll-free number (they will never call). Do the same for addresses. For phone, make sure you include all formats like 123-345-6789 and 123.233.2133, and so on. Double-check everything. Then, get rid of the e-mail addresses. Do a search & replace for “@realshop.com” and replace it by “@fakeshop.com”.

Ultimately, get rid of all occurences. Rename the folders that include “realshop” and replace it by “fakeshop”, and to a final search & replace in all the files for “realshop” and replace by “fakeshop”. This way, there should be no way to recognize that the shop is fake. You can change the logo at the top of the page, or if you are lazy, rename the logo file to another name and the browser will just put an “image not found”, it's not a big deal.

We are done with creating the shop. It might seem a lot of steps, but doing all that search & replace and preparation should take less than 5 minutes when you are used to it.

The next step is hosting your website. It is important that you use an anonymous host, so for this example, we will use Arvixe. 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.

It is also important that you change the WHOIS information to match the name you will be using on your Stripe account. Your web host will allow you to do that for free. Anyone can look it up on whois.net as this is public records. If the bank accout, shop and WHOIS are under different names, flags will be raised. Assign all 4 contact types to match the victim's information. It can be changed later and many times anyway.

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.

Before you open the account on Stripe, you should make sure you completely spoofed your VM. Also disable Flash plugin. Stripe has a very clever way of identifying you, which means they can identify

you even if you change IP and change browser. Better use precautions and see section 2.6 to completely appear as someone else.

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.
}
?>
```

For your convenience, I have included this file in the package, as well as the Stripe library package. They are hard to find on their site and I am doing you a favor by including them.

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 to be 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.

By experience, chargebacks take forever to arrive, and less than 25% of your transactions will end up in a chargeback. You shouldn't see a chargeback before at least 10 days, and probably more. I kept one of my old account, and after 2 months of inactivity, 38% of transactions had received a chargeback, so this is not something you should worry about.

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!

A word of advice though, I do not recommend using Ally or Netbank, as they often flag transfers coming from Stripe and lock the accounts. You should head to Evo and get a real bank drop, it might cost you a bit of money but it's worth the investment for sure.

By experience, Stripe looks at the domain age for your domain. You should wait a bit before you setup your Stripe account, or buy a cheap site on Flippa just to snag the domain name. This is not extremely important but can lower the flags even more.

Another way to get around fingerprinting and look more like new is to use a RDP. You can purchase some on the marketplace and they work pretty well for setting up Stripe account. Only login from that RDP and if the RDP dies, just don't log in Stripe dashboard anymore. You will still get the deposits anyway.

If the account gets closed, they often tell that they will refund charges to cardholders. If this happens, be quicker than them, and refund all the charges yourself. Refund everything you can. This way, you will be able to re-use those cards for another shop and you will save a lot of money. The cards will most probably not get burnt for fraud, because the charge was refunded. When you do that, however, wait at least 5 days before re-using them. This will lower the fraud score.

For UK carders, Stripe may ask for a scan of a government-issued photo ID at some point. It is a wise idea to make one when you start making some money with Stripe, so you can provide it when you get asked for it. It's not hard to make using Photoshop.

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 is registered 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 1st, 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 will probably 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.

Section 1.12 – Maxmind Fraud Prevention Algorithm

The most popular software used by merchants for fraud prevention is the Minfraud software, designed by Maxmind. It is used to keep fraudsters as bay, but their formula is not so secret. I will give you the formula, and explain the variables. There is a way to keep this score low.

Many stores have their own preset limits, which are not made public because each store is different. For example, a store can say that over 7 they send the order to manual review, and over 9 they cancel it. The definition of the variables goes as follow:

1. *IsFreeEmail*	Is the e-mail address from a free provider like Hotmail or Yahoo?
2. *CountryDoesntMatch*	Are the shipping and billing countries different?
3. *IsAnonymousProxy*	Is the user using an anonymous proxy like a VPN or blacklisted Socks?
4. *HighRiskCountry*	Is the order involving Ghana, Nigeria, or Vietnam? List updated often.
5. *BsDistance*	Distance between billing and shipping addresses, in kilometers.
6. *MaxEarthArc*	The half-circumference of Earth, currently set at 20,037 kilometers.
7. *BinDoesntMatch*	Is the BIN from a different country than the IP address used to order?
8. *BinNameDoesntMatch*	If user is asked for bank name, did he answer correctly?
9. *CarderEmail*	Was the e-mail used for fraud on other sites using Maxmind?
10. *HighRiskUsername*	Was the username used for fraud on other sites using Maxmind?
11. *HighRiskPassword*	Is the password the same than the ones used for fraudulent orders?
12. *ShipForward*	Is the shipping address a mail forwarding company?
13. *ProxyScore*	Is the IP address a proxy or socks?

The algorithm used for fraud score calculation goes as follow:

2.5 * IsFreeEmail
+ 2.5 * CountryDoesntMatch
+ 5.0 * IsAnonymousProxy
+ 5.0 * HighRiskCountry
+ 10.0 * min(BsDistance, 5000) / MaxEarthArc

+ 2.0 * BinDoesntMatch
+ 1.0 * BinNameDoesntMatch
+ 5.0 * CarderEmail
+ 5.0 * HighRiskUsername
+ 5.0 * HighRiskPassword
+ 5.0 * ShipForward
+ 2.5 * ProxyScore
= Maxmind score for this order

Now that you have this formula, let's see how we can reduce the score to almost 0. Although many stores use proprietary software, this one is widely used and is the most popular. Since there is no way of knowing which software the shop uses, just pay attention to all the variables and try to look legit. Here is a more in-depth explanation of each variable and how to pay attention to it.

1. IsFreeEmail

This variable is set to 1 if you use a free e-mail like Hotmail and Yahoo, so don't use it. I'll give you a trick. Remember the Stripe cashout part? Create an e-mail address from the same domain, like shopper.name@myfakeshop.com and use it. Since it's a paid e-mail, this flag will not be raised. I always did that for my orders.

2. CountryDoesntMatch

This variable is set to 1 if you ship to a different country than the billing address. This can be solved by using a card from the same country than the shipping address. This is easier if you ship to USA. Note that this is not a big deal since you can make an excuse, but let's not raise flags for nothing.

3. IsAnonymousProxy

This variable is set to 1 if you use a VPN or public anonymous proxy. This is also true for blacklisted socks. You can use a RDP instead, or if you can't get one, try to find a clean socks, but it's mostly trial and error.

4. HighRiskCountry

This variable is set to 1 if you have either the billing or shipping address in a country that is considered high risk. Since this list is always updated, I can't provide the list, but no western country is in that list, so if you are in UK or in USA, no danger.

5. BsDistance and 6. MaxEarthArc

This is the distance, in kilometers, between the billing and shipping addresses, up to a maximum of score 10. You can solve this problem by getting cards in the same state than you are shipping to. Using a California card to ship to New Hampshire will raise this score.

7. BinDoesntMatch

This variable is set to 1 if the BIN is from a different country than the billing address. This is the problem with non-AVS cards, and why I don't recommend them. Stick to AVS, and get a BIN from the

same country. Use common sense.

8. BinNameDoesntMatch

This variable is set to 1 if the user answers the question “issuing bank name” incorrectly. So for this one, do a BIN check, and write the correct name, exactly as it appears in your BIN info, and you will be fine.

9. CarderEmail

This variable is set to 1 if the e-mail address was previously used for carding. All websites send regular usage data to Maxmind and they have a list of the carder e-mail addresses. One mistake carders make is reusing e-mail addresses, thinking that shops don't know that the previous shop was carded. Maxmind holds a list of carder e-mail addresses submitted by shops. Use each e-mail address only once, and use a different e-mail next time you card.

10. HighRiskUsername

This variable is set to 1 if the username was previously used for carding. Read the above statement and do the same thing than e-mail addresses.

11. HighRiskPassword

This variable is set to 1 if the password was previously used for carding. Pay attention to not re-use passwords across sites.

12. ShipForward

This variable is set to 1 if the shipping address is a mail forwarding company. They include MyUS, Bongo, and many others. Some sites will outright ban those addresses and cancel every order made to them. Avoid shipping there, there are many other options to get drops.

13. ProxyScore

This variable is set to 1 if the originating IP addresses is a proxy, or a socks. If the proxy's goal is to be anonymous, then the variable IsAnonymousProxy will be set to 1 also.

Having all this information in hand will allows you to nuke fraud prevention systems and get your stuff even more easily. The high-risk country list is always updated but you can always google for it if you want to have an up-to-date list.

Always use a VPN with your socks proxy. The TrueIP technology used by many fraud prevention software can sometimes bypass your proxy and get your real IP, so pay attention.

Section 1.13 – Order Verification Procedures

The decision to accept or reject an order is based on many verification procedures that shops do, so I will make an entire section on that part so you can avoid cancelations. It's frustrating when you have a platinum card and you burn it. So read on.

Utility bill

Some shops will ask you to e-mail them a copy (front back) of a recent utility bill. Most of the time, they require the bill to be no older than 3 months. To deal with that, I have included a PSD file of an electricity bill, and the text of the name and address is editable so you can edit it at will without too many Photoshop skills. Make a bill with that PSD and send it along with the back image of the bill (JPG format). No need to make anything more complicated.

Scan of credit card

They can ask you to send a scan of the credit card used for the purchase. I have included the PSD of a credit card, with the same exact font used for real cards. Edit it at will, change the logo, and export to JPG. It is a wise idea to google for an image of your BIN (example, “platinum chase visa”) so see what it's supposed to look like. With the included PSD, this should be a piece of cake too.

Photo ID

It's difficult to provide scans because every state and every country is different. In that case you should just google for your requested ID, for example “michigan driver license” and edit it with Photoshop. The driver's license number can be made-up, because they can't verify that. Just concentrate on making the issuing and expiration dates logical, change the picture on the license, and put your name and address and it should be fine.

Phone verification – easy

They can call you for a verification call and just ask if the order is legit, and sometimes ask to confirm both addresses. This is fairly easy, and the order will go through.

Phone verification – hard

They can be more pissy and ask you verification questions. Those questions are all from public records and are included in your background report. If you did your homework and studied your background report, you will be able to answer them. They have multiple choices (4 choices), and most of the time, 1 question has “none of the above” as the correct answer. By memory, B&H Photo does this type of verification.This used to be a place where I like to shop, but since they increased their security, Geoffrey (the verification agent) is a bit more hard to convince.

Having shipping address on file with the bank

They can ask you to call your bank and make sure the shipping address is on file with them. Read the section about ATO and you will learn how to do that, it's not that hard, but you will need a fulls in order to achieve that.

This completed the list of verfication procedures used by online shops. Learn from this section, study it, and get ready for anything.
It your last order was easy, it doesn't mean that your next one will be easy. Some sites increase they security procedures for any reason and decide to be pissy.

You must usually respond within 24 hours to avoid order cancelations. Be quick. If you plan on doing a big heist, you might want to have the scans ready before you place the actual order.

Section 1.14 – Stripe Automated Cashout

In the new version of this guide, I have included a small piece of software made by myself: the Stripe cashout script. It allows you to send automated queries to your server. I will tell you how to use this little piece of engineering.

First of all, make sure your Stripe server is all set (see section 1.10 for that) and that you can make live charges. Make sure charge.php is uploaded and everything works. Good? Now let's make automated charges.

Open the cards.txt file and put your credit card numbers, dates, and security codes. If your credit card number is 4123 4567 8901 2345, expiration 04/2034 and code 343, the lines should be as follow:

```
4123456789012345|04|2034|343
4444444444444444|02|2019|123
```

One card per line. No extra characters, no spaces, nothing. Just card information in the cards.txt file. You can put as many as you want.

When you open launch.bat, you will be asked for 5 questions before the script starts to run. Here are those questions and how to answer them.

Q1: Charge.php URL
This is the full URL of charge.php on your server, without any extra parameters. Make sure the file is uploaded and that you can access it with your browser.
Example: http://www.myfakeshop.com/charge.php

Q2: Minimum delay between charges
Since charge times are randomized to avoid making an obvious pattern, this parameter is the minimum number of seconds to wait between charges. We recommend a minimum of 3600 seconds (1 hour) to avoid raising suspicion flags by Stripe. This parameter has to be an integer without any extra characters.
Example: 4400

Q3: Maximum delay between charges
Following Q2, this is the maximum number of seconds to wait between charges, and this number is inclusive. Again, no extra characters or spaces.
Example: 8200

Q4: Minimum charge amount
Charges are also randomized, so you need to supply the minimum and maximum amount of the charges. I recommend staying under $200 to avoid suspicion. This is an integer, is only the integer part, and must not have decimals. For example, 54 means a charge of $54.00 (or any other currency you might have put in your charge.php file) and this number is inclusive.
Example: 50

Q5: Maximum charge amount
Following Q4, this is the maximum amount (inclusive) of the charges. Again, try to stay under $200, and you should be fine.
Example: 140

The script will run for as long as your cards.txt file is not exhausted. Note that all cards are loaded at execution time, so if you add cards to your cards.txt file, they will not be taken care of before you restart the program. The log.txt file will contain all processed cards and the returned result (OK, declined, invalid, etc.) so you can exchange the dead ones.

There is no limit on the number of cards you can cashout, and if you use this piece of software in an intelligent way, you will avoid account suspension.

If you are familiar with command line, you can also launch it using command line:
```
java -classpath . app.Main Q1 Q2 Q3 Q4 Q5
```

This last method (command line) is useful when you have many servers to probe at the same time, for maximum profit. If you want to stay simple, just open launch.bat and supply the parameters.

No need to pay thousands of dollars for cashout software when you can just use this small script to do the job for you!

Section 1.15 – CC to BTC

Many people are also looking for CC → BTC methods. I will explain a few ones here, but be aware that some methods might not work anymore, or new ones be available. I try to keep it as much up to date as possible.

Method 1: Virwox

This is one of the most popular methods. Virwox is hard to card, but there are ways to do it. First of all, almost all Socks are blacklisted; you will need to use a RDP close to the cardholder's location. Create an account using an e-mail address that's not free, such as your Stripe fake shop e-mail address. Once the account is created, you should wait at least 72 hours before doing anything.

During that 72 hours, you will need to ATO the credit card account and change the billing number (you can still use that card for purchases after, so don't worry) as there is a very strong probability that the bank will make a verification call. Skrill is a high-risk merchant and, even for my legit account, I get calls from my bank when I use Virwox.

Then use the Skrill method to make a payment to charge this account, and stay under $100 for the first time. At this point, 3 things can happen.

#1: The transaction goes through and the account is funded. That's what we hope.
#2: Skrill asks for a SMS verification. You cannot use public SMS numbers, RingCentral numbers, or Google Voice. You need a real cellphone for that, and Skrill is very selective on numbers that they accept. You will need a physical burner cellphone to accept that SMS. When you do it, the transaction will go through and the account will be funded.
#3: The transaction is denied, at this point you will be happy to have an ATO'd account as you can call

the bank and authorize it, then retry.

Now that the account is funded, convert USD to SLL, then SLL to BTC, and make a withdraw to a bitcoin address you never used before. If a fraud is reported, that BTC wallet address will get blacklisted. You will then get a message that asks you to wait 48 hours before the withdrawal goes through. Actually, it takes in average 30 hours for the transfer to be complete.

You can now enjoy your fresh bitcoins!

Method 2: Coin.mx and Coinmama

You will need a fake ID, utility bill, and scan of the credit card to card those sites. Make sure you are good with Photoshop and that you can make them. You will need to ATO the accounts and be prepared to receive a confirmation call.

Since the policies of those sites always change, I will not go in the details of what they ask, but use your Photoshop skills and make some bitcoins using your cards.

Method 3: Carding things and selling them

This is the method most people recommend. Use virtual carding to card items such as electronics and sell them. Use the money from the sales to buy bitcoins.

Using eBay to sell carded electronics is safe. You do not need to provide the serial number of those items, so just sell them as if they are legit. Craigslist is also safe.There are many ways to get rid of those items, so just use your imagination.

Section 1.16 – Squareup Cashout

Sometimes, Stripe may not be enough for you, if you like to get greedy. You can take advantage of another method with even faster transfers: Squareup.

You will also need a fake website, just follow the same procedure than Stripe to create a fake but good-looking online shop. Go on www.square.com and open an account using the same information than your Stripe account.

Now, here's the difficulty. In order to process payments, you need the mobile application. They have iPhone or Android version, however there are cheaper ways than buying a burner phone. Also, burner phones can easily rat our your location with signal triangulation even if you use spoofers or any kind of gadget. For the sake of this tutorial, we will do everything on your computer. And I'll show you how to set up everything!

First thing, we will download Genymotion. Make sure you pick the latest version that includes Virtualbox. At the time of writing, this version is 2.2.2. Before you think about installing Genymotion, read on!

You cannot install Genymotion in your VM, it's simply not supported. The VM graphics card does not support OpenGL advanced features and no tweak will make this installation possible, so we will need to install Genymotion on the host computer. There is a way of protecting yourself.

First, turn on your VPN on your host machine. You will need to create a TrueCrypt volume for all that stuff, 10 GB should be fine.

Then, install Genymotion, use your TrueCrypt volume as the installation directory, and do not create any shortcuts. Open Genymotion and open the settings. Change all the directories to your TrueCrypt volume (example, Z:) and create a new virtual device. I recommend Samsung Galaxy S4 – 4.3 – API 18 – 720x1280 for best results. Make sure you can run your virtual device and that you can use basic Android functions (calculator, etc.). Where is the Google Play (the app store)? It doesn't come with the device. Fortunately, I thought about you, and I will show you how to add it! By the way, if you can't see that exact machine type, pick the closest type having version 4.3 of the OS.

Run your Android virtual phone, and drag & drop the Genymotion-ARM-Translation_v1.1.zip file into the phone. When prompted by a message asking if you want to deploy the archive, select OK. When it's done, reboot the phone. Repeat the same process with the other zip file, and reboot the phone. Now if you go in the main menu of the phone, you will see the Google Play store application. Now before you go crazy with Square, we need to do a bit of protection stuff before.

Create a Google Play account using fake credentials, any info is fine, it is not really important. Then download the Fake GPS app and use it to set your GPS location to the cardholder's house. It can be done just by dragging the map to make the dot above his house.

Download the GPS Test application and test some stuff to make sure your GPS location is correctly spoofed. Needless to say, a VPN connection on your host machine is also mandatory.

Once this is done, download the Square Register application and login using your created profile (fake fulls). You are now ready to accept manual charges! For each card, you just need to input the credit card number manually to process the charge.

Do not get too greedy with this method, maximum 4 charges per day. Funds should be deposited every 48 hours, so repeat this process until the account is burnt.

Since this runs on Android, there is no current automatic cashout script available like Stripe. However, inputting a payment takes 30 seconds of your time and is pretty straightforward.

The security measures of Squareup are very more lax than Stripe and can easily be defeated. If the method gets burnt for whatever reason, I'll make sure to update the guide with the newly found information. Also, deposits sent at 8PM PST. If you look at your interface around that time, you will see that the next deposit amount is $0. Do not get panicky, this is normal and stays like that for an hour or two, then everything goes back to normal.

I strongly advise against using any of your real life details on this Android device. Any LE officer with a subpoena can inquire Google to get your fake device ID and can match this with what Square got in file. They get quite a lot of details about your device so better be safe than sorry. You can always create a second legit instance of an Android device if you want to do real life stuff too, in fact you can create as many devices as you want.

On a final note, you can re-use your Stripe website to use Squareup, so save money. However, I advise against re-using your credit cards since a decline rate over 50% can mean an account closure. If you

use this method, use it the correct way and it will be a gold mine for everyone!

Also, I would like to add that Squareup has a threshold of $2,002 (I have no idea why $2,002 instead of $2,000, but life has decided so) per week for manually punched cards. They do not mention it in their terms of service, but any amount over that will trigger manual review such as requesting documents. You do not want that to happen.

If you get to a point where you get asked to provide ID, which is a probably idea after some time, there's no need wasting time photoshopping documents, as 90% of accounts get closed. Just give them no answer, and get a new account instead. Do not waste energy on this one. If this happens, just do like Stripe, and refund all the charge to cardholders as quickly as possible. You will be able to re-use those cards, but in another cashout method, not on Square!

I also discovered an alternate method that works well for Square in the beginning. Their cut-off time for deposits is 5PM PST. This means that all transactions made before this time will be deposited the same evening (and appear the next business day). When your account is new, you can start with 2 transactions daily, and for 4 days straight, make both of those transactions between 4:20 PM and 4:50 PM PST. They won't have time to place a hold on the account and your money will come the same evening without any problem. After 3 days, you should change your pattern because a “too identical” transaction pattern will trigger account verification. You can then do 3 transactions daily for 1 week, and then upgrade to 4 transactions. Add 1 transaction daily per week of account activity until you get burnt. Your dispute rate must stay under 5% to avoid account verification procedures.

When you start a new account, always change Android version (create a brand new emulator) and appear as new. New OS version, new phone type, and you should be fine.

Section 1.17 – Flint Cashout

This is yet another cashout method that works very well, because Flint is not yet wide known to carders. This is a company where you can make a lot of money! To get started, you will need:

- Full info (name, address, DOB, full SSN)
- Real bank account (banks like Ally don't work)
- Background report on the full info you have
- Android emualtor (look at the previous section to set-up Genymotion)

Go on flint.com and open a new account. You can re-use the same shop that you used for Stripe and Squareup. Use the same e-mail too. This way, your mere $7 for a month's hosting turned out to be a lucrative investment! Get your background report now!

This is because, upon submitting the application form, you will be presented with 3 verification questions. You can look at section 1.9 to get more information, as those questions are the same than TigerDirect asks. At least, they come from the same source, so you should have no problem, except that there is a secret rule that allows you only 1 minute to answer those questions, so it's not time to start looking everywhere. Be quick. You will know right away if you were right, because you need 3/3 in order for the account to be approved. If you fail, you will simply get a Sorry message and you wasted that fulls.

When linking your bank account, make sure the account is not a prepaid account. If you use a prepaid, Flint will silently accept it, and will hold your money forever. When you phone them, they will tell you to put another bank account. And when you do this last step, they will ask for documentation and scans / all the shit you don't want to waste your time with. So use a real account right at the start and you will avoid problems down the road. I learnt this the hard way, when my account with $3,000 got seized. I was quick enough to refund all the charges and re-use the cards on Square, but better keep it simple and get your deposits as planned. And remember that, their e-mail support will answer just when they feel like it. It's better to call them if you need help.

You will require the phone number, name, e-mail address, and dollar amount of last transaction when you call. Not very secure IMO, this can make ATO very easy for such accounts. If you want to be creative, you can find a merchant that uses Flint, and change their bank account to make the money flow in your bank drop instead. I recommend this only for expert users but it can be an additional stream of income.

Open your favorite Android emulator and install the usual Google Play packages (see section 1.16 about Squareup for this part), and you have a fully functional Android emulator again. You can also re-use the same emulator than Square if you wish.

Now, if you go in the Google Play store, you will see the Flint application, with a dreaded message saying that this application is not compatible with your device. No matter which emulator you use, you will get this message. I will show you how to get around it.

Put your emulator on the main screen, and look in the guide package for the .apk file of the Flint application. Just drag & drop it to your emulator's home screen and the application launch. Press the home button. Now go in the menu and you will see that the Flint application appeared in the application list. Open it, and login using your created account information.

At this point, before proceeding any transaction, you should link your bank account on flint.com if this is not already done. You require a real bank account, not a prepaid card or a shitty account. I will also point out that, placing money in a Ally account is about as safe as playing roulette, so I strongly recommend avoiding Ally. By experience, Bank of America accounts are the best for this kind of job.

Now that your bank account is linked, you are ready to start accepting payments. You should use the same rules than Square: avoid going over $300 per transaction, don't get greedy, and don't exceed 3 or 4 transactions daily. If, after 2 weeks, the account is still live, you can start increasing slowly, but I repeat again, do not get too greedy!

Everytime the account gets burnt, you need to create a completely new emulator, but it takes less than 5 minutes if you master your stuff, so don't be lazy. After all, people work all week and don't even make half of what you can cashout in a single day. Enjoy the chance you got, cashout slowly, and hug your cat.

Finding bank drops is relatively easy; I got several people asking me in private how to get a drop. This is very simple, there are many vendors on Evo, and even on the forum, if you post in the wanted section, you will see how many people have such accounts. I never had problem finding a cashout partner. You can expect a 50% share with the drop owner, unless you can get your own drops, but this is a harder job.

It is also important that you create a new Google Account everytime you make a new emulator. This way, you will avoid making your pattern traceable and you will look like new. You can use Square and Flint on the same emulator, and re-install both on another emulator once both of them are burnt. By experience, Flint accounts take long to burnt, I rarely had accounts burning before one week, so there is still a lot of money to make there. Payment processors are really a goldmine for people seeking to make money in the carding world.

The first deposit can take a few days to arrive; this is due to the fact that Flint has pseudo-random deposits, usually 2 days between them. This is a weakness of their system, but it's still a good money-making source. I had to e-mail their support the first time, to find out that the first deposit is always delayed a bit. This is not a problem, I always got a minimum of 2 deposits before getting an account burnt for high-risk activity, except for the first time (I had used a prepaid account, which is the worst thing to do, and they swallowed all the money).

Please avoid spreading those methods in the open. If you took the effort and money to buy this guide, you want to be able to fully enjoy your carding methods and make money without hundreds of newbies trying and failing and raising flags. It will become harder if too many people try those methods, so let's keep those tricks between people who purchased that guide. You don't want to cut one of your sources of income just to look good.

When exploring those cashout systems, it can be surprising to see how many lawsuits they must get from legitimate merchants who get their money seized because of security features. They still put that information in an obscure way in their terms of use, so legally they have the right to do that, but we just need to be smarter than them and look legitimate. After all, payment processor cashout has and will be always be a lucrative stream of income for people who want to make an extra income in the fraud scene without involving anything physical.

With all those cashout methods, whenever you feel like getting greedy and charging more, just think about this Chinese proverb with a lot of wisom:
“Is it better to see $100 in your bank account, or $500 in your blocked Stripe account?”

- Sage Alpha

Section 1.18 – PayAnywhere Cashout

This is a payment processor that gets very little fraud amount and is not yet aware of all the risks; try not to burn this one, as it is a goldmine as of now. Same principle that Flint, but easier to cashout. On the other hand, opening the account requires a bit of skill.

Get your SOCKS proxy ready, and VPN to protect yourself. Head to www.payanywhere.com and open an account. You will need a background report because you will be asked 4 verification questions. You must get 4/4 to get the account opened. If you fail, 4 new questions will appear, but this means you are already burnt. Try with another fulls and clean all cookies / user agent / etc.

For some reason, the verification questions are trickier than other sites, so it requires a bit of luck. If you want to be near 100% sure, you should card a credit report on Equifax or TransUnion. Once you are successful, the site will tell you to wait up to 24 hours to get your account. Just do it.

You will receive a welcome e-mail and you will now be able to log in your PayAnywhere online interface. Link your bank account, then wait 48 hours. You can now download the PayAnywhere

application on Google Play on your burner Android and start making charges. Stay under $200 for charges, and do not go over $1,000 per week, or you will fall in the audit category and will be asked for 3 months of bank statements.

At some point after a few successful charges, you will receive an e-mail asking you to call the merchant awareness department. You will be provided with a phone number and extension to call them, and you must have your merchant number ready. You will require the full name, last 4 of SSN, and merchant ID. You must also spoof the number to reflect the number you put on your PayAnywhere account. Do not be scared, this is only a welcome call. Here is how this call usually goes.

Agent: Thank you for calling Bancard merchant awareness department, my name is Bobby, may I have your merchant number?
You: 93932973423
Agent: Thank you, who am I speaking with?
You: Barack Obama
Agent: Thank you Mr. Obama, can you please verify the last 4 digits of your social security number?
You: 1234
Agent: Thanks. It was me who sent you this e-mail, the reason for this call is to help you get started with payment processing with us and wish you welcome to our services. I see you have already processed transactions, how do you like it so far?
You: I like it so far, the application is fairly simple and quick.
Agent: Glad to hear that. Also we wanted to explain to you the procedures for disputed and declined payments. (the agent will speak for around 1 minute explaining some key points)
You: I understand.
Agent: And in case we decide to put your account on audit, we will require more information about the cardholders. (other procedure explanations)
You: All right.
Agent: And what exactly is your business?
You: I sell skateboard accessories online, I am a reseller.
Agent: Do you have a business registration certificate, or do you do business under your own name?
You: My own name, Barack Obama. (it is important to answer that, otherwise you're screwed)
Agent: Thank you. And to finish, do you have a website address where customers can view your shop?
You: Sure, www.myfakeshop.com.
Agent: Thank you Mr. Obama, and do you have any more questions?
You: Nope thank you.
Agent: Thanks for returning the call following my e-mail, have a good afternoon!

And you're done. Stay under $1000 per week and deposits will come every 2 days. This way, you will stay under the radar and receive deposits every 2 days. It is an extremely lucrative cashout method, so use it wisely.

It is also a wise idea to write a small description for the charges you make, for example “Order 22178” so you look more legit. You can google “fake invoice generator”, there is a good generator out there that allows you to generate invoices. You will need Adobe Acrobat to get rid of the “generated by” text at the bottom, if the site decides to put a watermark.

Section 1.19 – Getting Asked For Photo ID

Sometimes, merchants can ask you for a photocopy of a government-issued Photo ID. This is easy to

bypass if you have the right tools, for example, not sending a JPEG image with the “Adobe Photoshop CS6” watermark in the file metadata. I'll tell you the secrets.

I have included a SSN Card with this guide. The card is in PSD format and is the exact same font than the real SSN cards. The “baseline” layers are the bottom of the characters. You can just copy and move the digits' layers to form the SSN, and for the name, use the provided characters. If you are missing some characters, I put a font layer in the PSD file. Just write it using that font, and put some black brush strokes and eraser strokes to make the letters look like the other ones.

For driver's licenses, the process is a bit trickier, but doable. Since DL templates always change and vary by state / country, it is impossible to include a scan, but you can search on Google Images for the template you are looking for. Get a high resolution image if possible. Once you found it, you will need to edit the information on it, the number too, and expiration dates. Try to find the Facebook profile of the victim to see if you can find a decent-looking photo, otherwise you can get a stock photo of driver license picture, on sites like iStockPhoto.com. Just card the picture you want to use.

For utility bills, I have included a scan of an electric bill. This template is very easy to work with. I also included the font you need to use for it. Edit the right information on the bill; this should be very easy to do. Leave the back as it is, we won't need to edit anything there.

Once you are done, save the image in JPG format. Do not send the file yet, as the Exif data of the image shows “Made with Adobe Photoshop CS6” and any smart merchant will spot that. Create a new OpenOffice Writer document, import the image in the document, and save it to PDF format. You can now safely send this PDF to the merchant, who will have no clue that you photoshopped the image. If your Photoshop skills are not so bad, you should pass verfication this way.

That's it for the first chapter! Making money is a good thing, but more importantly, you will need to protect yourself. That's what the second chapter will be about. Cashing out and avoiding LE can become a way of living if you like easy money. Let's move on!

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.

If you want to be paranoid about security, you can make a door protection for your computer. If you have your VM running in TrueCrypt and you have to leave your computer on while you're somewhere else, sleeping for example, it's a good practice to use an extension cord to power your computer, and arrange that extention to unplug when the door is opened. In case of a raid, all proofs will be destroyed. This is not mandatory but can be an additional layer of protection in case the police pinpoints your

location and decided to pay you a visit. But usually, when you leave the house or go somewhere else, you should at least unmount your TrueCrypt volume. If you don't want to lose all your VM status (sometimes you have several running applications), you can Save the virtual machine state on shutdown, to avoid re-opening everything.

If you started carding before acquiring this guide, and you installed carding stuff on a hard drive, do not simply erase the files. They can easily be recovered by any competent LE officer. To avoid that, download the DBAN software, and burn the iso to a CD or a DVD. Insert the CD in the computer, boot on it, and secure erase your hard drive using the DoD standard or the RCMP method. This way, you will erase all trace of files related to carding and you will be safe in case your hard drives or USB drives get seized by LE for investigation purposes. When they barge in your house, you will not have time to destroy all your hard drives. They take an average of 3 seconds to take what they want. Besides, you do really want to sleep with worries and be scared to get busted? Me neither.

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.

As soon as RingCentral receives a chargeback, you will be notified by e-mail and the account will be terminated. They ask for supporting documents, but do not respond. Just open another account with another card.

Section 2.3 – Spoofing Android Device – The Perfect Way

This section is one of the most important, if not the most important, if you want to have luck at cashing out big amounts. If your goal is just to make a quick heist and pull $1,000 then move to something else, it's all fine if you skip this section. However if you want to follow me and make 5 figures per month in fraud money, you definitely need to step up your game.

Stepping up the game means getting a physical Android device at your local shop, which will cost you around $100. You can also get a used one on Craigslist, in fact as long as you have a physical device in your hands you will be fine. You do not need to get any SIM card or any plan, just get the phone, you will not use it for calling anyway. However if you already use a physical burner Android device, you can re-use it for that.

This section is also about completely giving up on the Genymotion emulator, because it has too many restrictions and you will not be able to spoof it completely. Square and Flint applications have a lot of special permissions which include getting the MAC addresses, serial numbers, IMEI, IMSI, phone numbers, and a lot more information. This section will tell you how to spoof that data and send garbage (but real-looking) data to trick those applications into believing that you are someone new. If you follow this tutorial, there is no way that even the most advanced application in the world could find out that you are spoofing your identity.

Step 1: Unlocking and rooting the phone

First of all, prepare your phone, connect it to a VPN (any is fine), create a junk Google account (any name is fine, it doesn't matter, but don't put your real name), and download the IMEI.info application. You will only need this one for now.

The next step is unlocking your phone's bootloader. Since every Android phone model is different, I can't provide exact instructions, but I will put you on the right path for some of the major brands. I have included the ADB and Fastboot folders, in case you need to use any of those files during the process.

Motorola Devices
Head to http://motorola-global-portal.custhelp.com and you will have all the required instructions. The website is well done and you should find it easy.

LG Devices
Head to http://forum.xda-developers.com/showthread.php?t=2224020 and you will see the instructions, it's not very hard to.

Samsung Devices
There are too many different models, and every model is different, you can just search for it. Most phones can skip this step too and proceed directly to the next one.

Now that your phone's bootloader is unlocked, you will need to root your phone. This varies by device, but I will give you the usual procedure. The normal procedure is more complicated, but I created batch files to make it faster, for your convenience.

Plug your Android device in the USB port, and put the “UPDATE-SuperSU-v2.02.zip” (from the “Android ClockworkRoot” folder) at the root of the phone's SD card. Shutdown your phone, and power it on again while holding the “volume down” key and you will be in the boot menu. Then double-click the “ROOT.bat” file from the same folder and it will install the recovery ROM. Boot the phone in recovery mode and you will be in the Clockwork boot menu.

From there, install a package from the SD Card, and browse to your SuperSU file (the zip file we put earlier) and your phone will be rooted. Optionally, if you want to restore your logo and get rid of the warning message when you power up your phone, you can search for your firmware, download and unzip it, replace the “logo.bin” file in the provided folder by the one you downloaded, put the phone in boot menu mode, and double-click “LOGO.bat” to restore your logo.

Now your phone is rooted, but that was only the first part. Now we will install the spoof tools that will allow us to become somebody else without anyone noticing. We want to make money, so let's do it the right way. Optionally you can download the “Root Checker” application from Google Play to verify that you correctly rooted your phone.

Step 2: Installing Xprivacy package and framework

Boot your phone in normal mode and put the “xposed.apk” and “xprivacy.apk” files at the root of your SD Card. On your phone, open Google Chrome and go to the address “file:///sdcard/xposed.apk” and this will download the Xposed Framework. Go in your Downloads folder and install that file. Once it's finished, reboot the device.

Repeat the process but for the “xprivacy.apk” file. You will then need to open the Xposed application, enable the framework, and enable Xprivacy. Reboot the phone again. Xprivacy is an operating system modification that allows you to send fake data to applications who request device data like IMEI, IMSI, serial, and a few more parameters. We will use this one to trick applications into tricking that we are somebody else.

Connect to your VPN (Android has a native VPN function in the Settings menu), open Google Play, create a dummy account, and download (but do not open) your favorite payment applications like Square, Flint, PayAnywhere, etc. and install them on your phone.

We are finished with application installations, now we will proceed to the spoofing part. This is the most interesting and the most important part.

Step 3: Spoofing the application privileges

Be careful in this part. Doing a mistake can result in your identity being revealed, so follow carefully. I assume no responsibility for anyone getting busted because they incorrectly followed the instructions. You have been warned. Unplug your phone from your computer before proceeding.

Open the Xprivacy application and click the icon at the top-right of the window, then go in Settings. There will be a “Randomize data” button, click on it. You will see below that the IMEI, IMSI, serial, etc. have been spoofed. You can click as many times as you want, it's all fine. Uncheck “Randomize data on boot” and make sure nothing is checked beside the parameters. Click on the Phone Number field and put the 10-digit phone number of your target, and put the latitude and longitude of the victim's house. Exit the settings menu.

You are on the main screen of Xprivacy. Check the box on the right of your application, and click on the application icon to open the advanced properties panel. You will need to check the boxes beside all elements that have a small key icon beside, except Internet. Do not check the boxes if the background is red. Last but not least, make sure the “Restrict” option at the top is set to On.

Congratulations, your device is spoofed! But there is one more detail: having a legitimate IP is a must. So we will move on to the last part of this section.

Step 4: Connecting your device to SOCKS proxy

First of all, you will need to configure your router to use a VPN connection. Any VPN provider is fine. The same procedure will be detailled in section 2.2 (burner phones). Configure PPTP as the WAN connection type, and on your PC, google “what is my ip” to make sure you are behind a VPN.

On the computer (or virutal machine) where you are using VIP72, configure the firewall to allow incoming TCP port 9951 always on all domains. Make sure you open VIP72 client and Proxifier and test your connection to make sure you are appearing at the proxy location.

On your Android device, head to Google Play and install ProxyDroid. Open the application, and put the local IP address of the computer (or VM) running Proxyfier, port 9951, no username nor password. Check the “global mode” and connect the proxy. Your phone will vibrate and make a sound, and you will be connected to the proxy.

Open Google Chrome on your device and search “what is my ip”, at this point the displayed IP should be the IP of the proxy you are using. You will also appear at that location. It is now safe to open your payment processing application. Garbage data will be sent to those applications instead of real data, giving you total protection.

Your accounts will take a very long time to get burnt; this method is a proven spoofing method found nowhere else than this book and is sure to take forever to get burnt. You will notice that some application options will get blocked and Xprivacy will display a message; for example, Square wants to record audio from your microphone, which is a privacy invasion. Flint wants to read data from the computer connected via USB; hence the importance of unplugging your device.

Section 2.4 – 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 2.5 – 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.

About 1 year ago, I landed in Japan, and when getting out of the airplane, still in the boarding dock, there were 2 security men blocking the way. They shouted, “everyone get your boarding pass out!”, and people passed one by one, “okay”, “go ahead”, until there was a weird-looking guy who showed his pass and the bouncer said “follow me”, as they were going away, the security shouted, “everyone else can go!”. If you don't want to be this guy, read on.

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 wait for 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 always welcome to remind our fellow carders. To have a strong story, create a bitcoin wallet with a random name. Create a new Virwox account with your real details, buy bitcoins for around 30% of the flight value, and send them to that fake wallet. Then, create a fake e-mail address under that same person's name, and exchange with your real e-mail like if you are negotiating a fare of about 30% retail price. Once your flight is over, use the bitcoins in that wallet as you wish. In case you get pulled over at the airport, you will be able to show those e-mails and transactions and act like an innocent vitcim. If you booked through a third party though, the chances of that happening are very low.

Also, ATO is required for flight tickets over $300 as most sites will call the billing number to verify and they will cancel the order if you are not available to pick the call, so have your burner ready if you do that.

Section 2.6 – Spoofing E-mails

Sometimes you might need to impersonate someone and spoof an e-mail for various reasons. There's a clean and undetectable way to do that, and that's what I'm going to explain here. The e-mail will look 100% legit.

To spoof e-mails, you will require to make the e-mail yourself. This means creating the headers and everything. To make a test, just send a "Hello World" to a test Hotmail address, click on "View Message Source", and you will see the top headers. Paste everything (the source) in a Notepad++ document. You will see a header that looks like:

```
From: Real Name <realname@tcf.onion>
```

Modify it to the one you want to show, it's pretty self-explanatory. For example, change it to that:

```
From: TCF Hack <tcf@tcf.onion>
```

Then you have the full e-mail in a Notepad++ document. Next, get a Telnet client. I recommend Putty, it can be downloaded for free. Next, make sure you use an anonymous connection (I advise against VPN as it is obvious it's coming from a public proxy; use something like a hacked wifi, 3G dongle, etc.) and your security is correct.

Find the mail exchange server for your domain. For that, go on http://www.dnsqueries.com/en/mx-lookup.php and enter your domain, example "hotmail.com" and you will get the mail exchange addresses. If there are many, just pick one random. In your case it will be "mx3.hotmail.com".

We have everything we need! Open a Putty Telnet connection to your mail exchange server, port 25. The "conversation" will go as follow (it can vary a bit, depending on the messaging software):

```
Send: EHLO mx.spoofedserver.com
Response: Welcome mx.fakeserver.com
Send: MAIL FROM: spoofedemail@dsfdsagsdg.com
Response: 250 2.1.0 Ok
Send: RCPT TO: destination@fdsgsfdg.com
Response: 250 2.1.5 Ok
Send: DATA
Response: 354 end data with <CR><LF>.<CR><LF>
```
(paste all your data here, the one you edited with Notepad, then press Enter, put a dot (.) and press Enter again)
```
Response: 250 2.0.0 Ok: queued as 43958340634
```

Your fake e-mail is sent. Note that for some providers like Hotmail, if you attempt that (from Hotmail to Hotmail), they will put it in Junk Mail because the originating IP is not one of Hotmail's servers and they recognize it as spoofed. However if you send an e-mail to Hotmail from another server (example @tcf.onion), it will work like a charm. For smaller messaging servers, everything will go smooth. Now more people will fall for your scams.

Section 2.7 – Completely Spoofing Your Identity

This is about people who are serious into hiding your identity. Newbies would assume that by changing your VPN location, you are someone new. More advanced users will say that by changing your VPN, your Socks, and by using a completely new browser with user agent, changing fonts, resolution and systme time, you are better. In fact, both are wrong. Payment processors and Paypal have extremely advanced ways to fingerprint people and we will learn here how to bypass that.

What software or websites (through complex Javascript calls) can use to fingerprint you can include motherboard serial numbers, system UUID (unique identifier), and so on. That's a lot of stuff to spoof! To spare you the research of spoofing everything, I have prepared a small program, DMI Spoof, included in this package. This program was written by myself and is used to modify a VirtualBox virtual machine to make it appear completely new!

Run DMI Spoof and you will be asked for 2 parameters.

1) VboxManage.exe path. This is the full path of the VboxManage.exe file, usually located in the same installation directory than VirtualBox.
2) Name of your VM. When you open VirtualBox, this is the name that appears in bold black characters in the list. You know what this is.

Note that you can also supply those parameters at the command line to run it faster, the first parameter will be the VboxManage.exe path, and the second paramater will be the VM name. It provides a faster way to spoof everything.

Once you supplied those 2 parameters, DMI Spoof will alter the VM to change the BIOS brand, motherboard information and serial numbers, CPUID information and a few other parameters. You will appear as having a completely new computer made of completely different hardware, with no way of knowing that this has been spoofed.

Once you boot into your VM, change the following settings in Windows, as they can also be used to fingerprint you, and cannot be altered using DMI Spoof:

- Screen resolution (you can usually drag a corner of your VM)
- Install or delete a font in the Fonts folder (font list can be found using JS)
- Change the computer name (requires reobot)
- Use Tmac to spoof the network MAC address (can be found using advanced Javascript)
- Disable Flash (some sites silently place Flash cookies on your computer)
- Change user-agent (use the User Agent Switcher extension for Firefox)
- Change VPN location or Socks proxy (this is obvious)

Once you changed everything, do not re-access your sites from the same IP than before, or you will have to restart the whole process!

This is enough to protect you from all fingerprinting processes; for payment processors and high security sites, this is a must. There is no such thing as “too much security”.

Note that all this stuff is equivalent to getting a new computer. You will appear as completely new and there is no way to trace this back to the original machine. Spoofing DMI is something easier done on a virtual machine, and if you read this chapter correctly, you know that you must always place your carding software in a virtual machine for maximum security.

Section 2.8 – Safeguarding Your VPN

When it comes to using a VPN, many people have a sharky connection and their VPN connection disconnects sometimes. What happens if you are using an auto-cashout script or you are logged in using your fake username on an online shop? That's right. The connection will be established and will reveal your real IP. For Windows 7+ users, there is a Windows-native protection you can use to avoid such a thing.

When you connect your VPN the first time, Windows will ask you if this connection is Home, Office or Public network. You must select Public. Then go in the Windows advanced firewall settings and follow these steps to protect yourself:

1) Go in the “outbound traffic rules” section of the advanced configuration window.
2) Right-click on “outbound traffic rules” and select “add rule”.
3) You will be asked which type of rule you want to create. Select “program”.
4) Click on “browse” and select the .exe file of the application you want, for example Firefox.
5) Select “block connection”.
6) When asked when will the rule be applied, check “home” and “office”, uncheck “public”.
7) Give a meaningful name to this rule, for example “VPN Firefox”.
8) Create the same rule for every program you want to safeguard.

This way, all connections not on the Public domain (not made through VPN) will be blocked for the

selected programs, while still allowing the system requests to take the standard way. If your VPN is disconnected, you will not be able to use those programs. You should do this for:

- Firefox
- Google Chrome
- Tor Browser
- Tor Process
- VIP72 client
- Proxifier
- Pidgin
- Thunderbird
- Any other program you might judge useful.

Note that you can't just block every single packet not sent through the VPN. Many programs including the operating system itself must communicate on the local network without restrictions, and using the rule “block all programs” instead of selecting a program can make the system instable and have unpredictable consequences. Also, you need to use traffic on the “Home” domain to be able to connect to your VPN.

This ensures that your IP will never be revealed in case of a disconnection. In that case, just reconnect your VPN and everything will continue as normal. You will not have to constantly watch your connection status.

In case you do not know the path of the file you should choose, you can open the task manager using Ctrl + Alt + Delete (or right-click on the taskbar and select “open task manager”), right-click on the process and select “open file location”. This will give you the full path of the file, so you can add it to the firewall rules.

For older Windows versions such as XP, you can use Comodo firewall to achieve the same thing, however this is beyond the scope of this tutorial and has proven to cause system instability. The Windows 7 native method has proven to be the most stable and most secure as of now, so enjoy your protected system!

Section 2.9 – The 10 Most Common Mistakes

This section talks about the most common mistakes newbies make when they start carding. Some can be fatal, other one are just not important, but it's important to understand those points.

#1 – Bragging about your stuff

When you get free stuff, do not brag to your friends, your family, or girls. You never know when someone will be pissed at you and decide to report you. Keep it for yourself, and be quiet about it! Just say you have a way to get cheap stuff, and it's private. That's all.

#2 – Linking to your personal life

Do not ask a friend to use his house as a drop. Do not ship to your workplace, your dad's house, or worse, your own house! If the police shows up at your friend's house, he will rat you out for sure. Don't trust people that much.

#3 – Starting too big

When you first start carding, do not attack merchants like Newegg or TigerDirect. They are not easy and they will give you a negative feeling about carding before you even get free stuff. Start small, for example, clothes.

#4 – Using the same nickname on hacking boards and on clearnet sites

Many newbies forget that, and yes, there are probably LE officers on TCF, watching what's going on. If they can Google your username and see your Facebook or anything else, you're fucked. Use a name that you use nowhere else!

#5 – Responding to allegations of fraud

Sometimes, you can get caught off-balance, and for example, a shop will respond by "the order was fraudulent, so we canceled it". If you carded them successfully 3 times before, don't talk about it. If you just want to show them that you owned them, it can persuade LE to track you, because you just linked the fraudulent orders together. Just don't reply anything.

#6 – Not washing your bitcoins

If you buy (or card) bitcoins with Virwox, they can use the blockchain to trace where those bitcoins went, and eventualy link to you. Use a service like BTC Fog to wash them and get brand new bitcoins, not linkable to you, for your underground operations.

#7 – Talking to your partners on a traceable site

Do not use Facebook to talk to your partner about carding. Any LE officers can subpoena Facebook to get your conversation history and catch you. Use Pidgin + OTR to encrypt your conversation, and use VPN to connect to ICQ. Make sure you're not traceable.

#8 – Getting caught off-balance during an ATO

When you are ATOing an account, stay calm, do not get thrown off by questions. If you answer incorrectly (because very often, they have inaccurate information), stay calm and explain yourself, remember, the card is yours. Do not show fear, because they will catch you.

#9 – Hitting the same drop

This is pretty self-explanatory; finding drops is a pain, but make the extra effort and get a virgin drop. There is already heat on the first place, so do not put more and risk getting caught. A drop is good for 3 days; after that, time to move on. You can apply this principle with girls too.

#10 – Accessing your fake e-shop without VPN

When your Stripe account gets burnt and they subpoena your fake e-shop to give them the access log, you don't want them to see your real IP and trace back to you. Always use VPN to upload files, test your shop, and so on.

Section 2.10 – 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.

Conclusion

I hope this guide was useful to you. I tried to put as much as my knowledge as possible to help fellow carders in the underground world. Use any part you might find useful to you and try to hit for big. Again, thanks to everyone who bought the guide, and if you have any question, post in the forums so everyone can see question and provide better help.

I do not like to be PM'd with carding questions; the reason is that sometimes there might be a member knowing more than I do on a particular topic and if everyone can see your question, you can get more help, and it benefits to all the community. This is why I encourage you to make your question public.

Also, I do not provide personal support on ICQ. This guide has sold in over 300 copies and if I would help everybody who bought it, I would spend all day doing that. This being said, thanks for buying this guide, now time to make money!

Alpha02