

**FREE YOUR MIND**  
**<http://freeyourmindonline.net>**

**Can You stop Identity Theft?**

Today I would like to explore the subject of identity theft. It is the fastest growing crime in America. Identity theft can be one of the most devastating things that can happen to you and it can take years to resolve (trust me, I know). So we will go through some steps to try to avoid this.

It's funny how when you watch Tell-lies-vision, they make identity thieves out to be these geeks with 500 IQ's who can hack into virtual systems and get your personal info. The truth is, all you have to do is go to a site like [www.zabasearch.com](http://www.zabasearch.com) and put in your name and they can get all of your info. Now, you can send an e-mail to [info@zabasearch.com](mailto:info@zabasearch.com) and they will tell you all the hell you have to go through to hide the info, but there are plenty searchable databases out there where you can get info for a fee. This is the world we live in.

So what can be done to stop this madness?

This is a great article written by Jay Peters of the Credit Secrets Bible.

**How to Make Yourself Virtually Identity Theft PROOF  
in 60 Minutes or Less**

*By Jay Peters*

The FBI has called it "The fastest growing crime in America." Close to 10 million Americans every year are victimized by it and the costs are estimated at 50 billion dollars annually. Many criminals get off easy while the victims spend years working to restore their damaged credit reports and reputations. Worse yet, there seems to be no end in sight.

"The popularity of the crime is simply growing faster than the solutions to stop it", many experts conclude. The task of recovery is so time consuming and tedious, that multiple states have resorted to creating "Identity Theft Passports" for victims in an attempt to ease the pain for them as they endure the lengthy and frustrating clean up process.

By the end of this article I will share with you the secrets of making yourself virtually identity theft proof in 60 minutes or less (for free). I use the term "secrets" because less than 1% of the country is aware of these techniques (let alone practicing them).

If Americans took these preventative steps, up to 99% of all identity theft would be eliminated. However, “why” this beneficial approach is not being made common knowledge in the mainstream media is something I will not disclose in this article (more on that another time). For the moment, I believe the biggest crime one can commit is to not share this information with their friends and family (by the end of this article you will understand why).

Unlike other authors covering this subject, I will not insult your intelligence by sharing common sense tips like “Don’t carry your SSN Card or ATM PIN# in your wallet or purse” or “Keep all data sensitive documents like credit card and bank statements locked up in your home or office”. This is elementary advice at best. The key to protecting yourself from identity theft is to look at what the masses are doing and then do the opposite (to say the least).

Almost 70% of Americans are now shredding all their mail and documents and many are even subscribing to credit monitoring services or buying identity theft insurance in an attempt to protect themselves from becoming victims. While this is better than doing nothing it’s a far cry from TRUE security.

### **Study The Past To Predict The Future**

Contrary to popular belief, statistics show the majority of identity theft does NOT result from the internet as most consumers have been led to believe. In fact, less than 10% of identity theft cases (where data compromise can be determined), originated online. In almost 50% of cases, consumers are the ones who detect the breach. In nearly 40% of cases, the criminal was someone who was in close contact with the victim (*friend, relative, neighbor, coworker, in-home employee, waiter/waitress or financial institution employee*). In the end, nearly one third of identity theft cases come from a stolen wallet/purse, checkbook or credit card.

More interestingly, the age of the primary victim has lowered. If you are between the age of 25 to 34 you are now the largest target for the crime (65+ has become the smallest). The bad news is that while identity theft nationwide is on the decline (8.9 million victims last year down from 9.3 million in 2005), the dollar amount per victim is going up (\$6,383 last year, up from \$5,885 in 2005), and so are the number of hours victims spend cleaning up the mess (40+ hours last year, up from 28 hours in 2005).

We’ve all heard the saying “An ounce of prevention is worth a pound of cure”. Yet, no one is practicing it in the pandemic of identity theft. Credit monitoring is nice but only 11% of consumers ever catch identity theft through this means. Identity Theft Insurance (according to many experts), is even more of a hoax. It is a product marketed by playing on the fears of American consumers which does nothing more than assist them in cleaning up the mess only AFTER their identity has been stolen.

### **A Different Approach**

The following is a completely different approach to preventing and protecting yourself from identity theft. It is based on the reality that we live in a world now where there is zero privacy of personal data, meaning that your name, address, phone number, social security number and date of birth (even your mother's maiden name) can be obtained by ANYONE for a fee.

If you're one who feels this is paranoid thinking let me tell you about Amy Boyer. In 1999 Miss Boyer had an old high school classmate (Liam Youens) come back into her life many years later. Mr. Youens obtained Amy's SSN and other personal information after paying Docusearch Inc. \$150. After Youens shot Miss Boyer to death he then turned the gun on himself. Today the company tells visitors to its website that "not all searches are available to the public" and some are reserved for the investigative and legal industry. *How's that for homeland security?*

With this "different" approach we break down identity theft into two distinct categories. 1.) Basic Identity Theft. 2.) Credit Hijacking. By definition "Basic Identity Theft" is when the perpetrator steals your identity and then uses it to obtain NEW credit accounts for their personal gain. "Credit Hijacking" falls under a criminal stealing your identity in order to access and use your EXISTING credit accounts. Each type of fraud is different and therefore so is your plan of defense.

**BASIC ID THEFT DEFENSE:** The best proactive defense against basic identity theft is through the placing of an "Initial Fraud Alert" on all three of your credit reports. This "Initial Fraud Alert" accomplishes three important factors: 1.) Your name and personal information can no longer be sold by the credit bureaus to ANY third parties for any marketing purpose (*i.e. credit card offers, loan solicitations or credit pre screenings*). 2.) No one can be approved for credit with your personal information until the creditor personally calls you at the telephone number you list on your consumer credit report. And, 3.) Requesting this initial fraud alert entitles you to a free copy of all three of your credit reports (*one copy from each of the three major credit reporting agencies*). Please be advised that this is an "Initial Fraud Alert" which lasts only 90 days. To extend the fraud alert and obtain the above mentioned benefits for 7 years you will need to write to each credit bureau at the address provided within your initial fraud alert confirmation letter (*Note: It is likely credit bureaus will make the extended alert harder to obtain as a great deal of their revenue comes from the third party rental and sale your information*).

**CREDIT HIJACKING DEFENSE:** Most online merchants now utilize a security feature known as "Address Verification Service" or "AVS". AVS is a security feature for online merchants allowing them to only authorize credit card transactions for merchandise to be shipped to the same address which appears on the consumer's credit card billing statement. If the address does not match that of the credit card billing statement the transaction will automatically be declined. In other words, if someone gets your credit card number, expirations date and CVV code (the three digit code on the back of the card) the only way a transaction can be authorized online is if the merchandise is shipped to the SAME address that your credit card billing statement is currently sent to. This is what makes credit hijacking so dangerous. When a criminal hijacks your credit

they call up the banks (posing as you) and change your address on your credit cards with your personal information (i.e. last for of SSN and mothers maiden name) as if you were moving. They then proceed to order thousands of dollars in merchandise (online or over the phone) to be shipped to the “new” address. Because they changed “your address” on your credit cards they will bypass the AVS security from online merchants and the charges will be approved.

The only real defense against credit hijacking is to establish a personal security code with all your bank accounts and credit cards. This is a form of security which goes beyond your SSN, Zip Code, Date of Birth or Mothers Maiden Name to give you a whole new tier of personal security. This is a unique number or group of letters and numbers which you create and give to every credit card provider you have. For example. The number could be as simple as “JACOB2801” which is a combination of your best friend as child and the numerical address of the home you lived in growing up. By establishing this auxiliary passcode with all your credit card providers no one will be granted access to your accounts without the passcode being provided to them. Since you are the only one who knows it and it is nonpublic, it is truly secure. I have yet to find a credit card company which will not allow you to create such a passcode, an added layer of security.

### **Summary**

So now with the initial fraud alert established on your credit reports (and later extended), as well as the personal security code set up with all your bank and credit card accounts, you are virtually identity theft proof in under 60 minutes for free. Sure, someone can always “steal” your identity but the real joke will be on them. If they try to open a new credit account anywhere in the country the creditor is going to have to call YOU at the phone number listed on your report before it can be approved and it’s GAME OVER. If they try to hijack your credit by changing the address on your credit accounts they will be asked for not only the last four digits of your SSN and mother maiden name, but also your personal security code which they will NOT know and again it’s, GAME OVER.

Please understand that this article deals only with the topic of "financial" identity theft which is by far the most prevalent today. However, you should be aware you also have the following "seven MAJOR" identities in computers across the nation which are your: 1.) Driving Records/History (DMV Databases). 2.) Medical Records/History (Medical Information Bureau Database). 3.) Social Security Records/History (SSA Database). 4.) Insurance Claims/History (C.L.U.E. Database). 5.) Criminal, 6.)Legal and 7.)Public Record databases from birth records and real estate deeds to corporations, trusts and court cases. Yes, we are in the information age but all information is stored in databases. I think we are now living in the database age.

### **10 Extra "Financial" Identity Protection Tips**

1.) Keep a list of all credit card and bank account numbers with bank phone numbers so in case of loss or theft they can be notified immediately. 2.) Use only one credit card for

personal expenses and one card for business expenses and monitor accounts online weekly. 3.) Always send or receive mail only through secure and locked mail boxes. 4.) Never give out any sensitive information (SSN, Acct #, Pin #, Password Etc) via an email solicitation. Always type in and visit the website directly. 5.) Limit the information on your checks to your first initial, last name and address (nothing more). 6.) On all credit cards instead of signing your name write "Check ID!". 7.) Never use a debit card or Visa/Master Check card, as recovering fraudulently accessed funds from these accounts can be extremely difficult. 8.) Store all credit cards, bank statements and passports etc in a secure and locked place. 9.) Never give out your Social Security Number, Drivers License Number or Date Of Birth unless they have just cause and really need it. 10.) For details about establishing and initial fraud alert on your credit reports visit:

[www.experian.com](http://www.experian.com), [www.equifax.com](http://www.equifax.com), [www.transunion.com](http://www.transunion.com)

This and much more valuable information by Jay Peters can be found in the Credit Secrets Bible (in print since 1994). <http://www.creditsecretsbible.com>

To add to this article, there is also a company called [www.lifelock.com](http://www.lifelock.com) that implements the fraud alert for you. Now you obviously can do this yourself for free (they charge \$9.95/mo). But unlike Jay Peters, who says that this alert can be done for 7 years, they "claim" that there is no time limit and that they can do it forever. I called them myself. They also insure up to \$1,000,000 in damages if your identity gets stolen (which you should never need anyway if you establish your own passcode)

Also, if you do institute the fraud alert method, this will stop you from getting credit offers in the mail. Is this good or bad? Obviously good right? Well if you have oogley credit, and you are trying to improve it, then credit offers may be to your advantage. If this is the case, then a credit monitoring company like [www.identityguard.com](http://www.identityguard.com) would have to do. Even though this isn't very effective, it is better than nothing.

There is another technique you can use (if you aren't using the fraud alert method). You can use disposable credit cards. This allows you to create an account number for one purchase and then dispose of it.

American Express offers disposable transaction numbers. Discover card offers a "desktop virtual credit card." Citibank has a virtual account numbers program. You can also go to sites like <https://www.3v.ie/> to go virtual.

Hope this has been helpful.

So until next time,

Free Your Mind.

Cordially,

Matt Mason

For more resources, go to the Resource Center

<http://freemindonline.net/resources.html>