



7 Things To Leave At Home

By Miguel Barnes

©2013 MABCO Enterprises LLC -- All Rights Reserved

INTRODUCTION

The news is all over the media these days “identity theft is on the rise”. And it doesn’t matter who you are, you can still be a victim. Recent identity theft victims include Donald Trump, Michelle Obama, Joe Biden, Jay-Z and others. The truth is anyone can be a victim!

Identity thieves are becoming more and more clever in the way they are stealing our identities; coupled with the fact that a growing number of companies are digitizing their information and storing them in large databases. It is easy to see that the potential for identity thief will continue to rise for the near future.

Identity theft is a serious crime – one that is occurring with an alarming frequency. The statistics are mind-boggling.

- 1 in 4 US households have been victimized
- 10 million people last year affected
- Loss to businesses tops \$47.6 billion
- Loss to victims about \$5 billion
- Each victim spends about 30 hours trying to restore their name.

So what can you do to minimize your risk of having your identity stolen? Well you can start by making it harder for the identity thief to get your personal information.

Below we will look at 7 things that you should not carry with you. By not carrying them with you and keeping them

in a secure location, you will minimize your risk of having your personal information fall into the hands of an identity thief.

The issue of becoming a victim of identity theft sometimes is more the emotional impact and the time and effort needed to restore your identity and good name. Another good reason why you should be proactive in protecting your identity.

By protecting your identity, and putting a plan in place of how to restore your identity in the event it is stolen, you can have peace of mind knowing that you are prepared for whatever may come. With that knowledge you can also help those around you protect their identity as well.

Don't let the fear of losing your identity keep you in a state of inaction. Learn and put into practice what you learn and you can fight back against identity theft!

One: Social Security Card

Your Social Security Card is like gold in the hands of an identity thief. With your Social Security Number, they can open accounts, apply for a loan, obtain employment, file for a tax refund, purchase a home or vehicle in your name, and more.

Take the time to memorize your Social Security Number and leave your Social Security Card in a secure location.

Two: Too Many Credit Cards

Do you really need to keep all of your credit cards with you? My guess is that you probably don't. Keep one or two credit cards with you and leave the rest in a secure location.

It is also a good idea to copy or take a picture of the front and back of your credit cards and store it in a safe location.

Also keep your credit card number and their company's phone number safe but where you can easily access it. In the event that your credit card is stolen, you want to act quickly to freeze or cancel the account.

Three: Passwords/PIN codes

Some of us have fallen into the habit of writing everything down instead of memorizing the information. If an identity thief gets a hold of your passwords or Personal Identification Number (PIN) codes, you have practically given them access to your life.

Most people make the mistake of using the same Password and PIN code for all of their accounts. You should use a

different password and PIN code for each of your accounts. You might be wondering, how in the world am I going to remember all of those passwords or PIN codes? That is a valid question. You should take the time to come up with a system. For example replace common letters of your password with a symbol i.e. a = @, O = 0, L=1, etc. Your system should allow you to come up with unique passwords or PIN codes but also give you a way to remember your password or PIN code.

If you must keep your passwords and PIN codes with you, store them digitally in a password protected device.

Four: Checkbook

This might be a challenge for some people that are more comfortable using checks as a payment method. The issue is that your checkbook has many items that are of value to an identity thief.

With your bank account and routing number, an identity thief can order checks in your name but have them mailed to another address. Usually your checks will also have your address and phone number on it. The identity thief might also gain access to your signature.

Get into the habit of only taking your checkbook when you need it and not keeping it with you all of the time. Or if you know you are going to need a check, peel off one check out of your checkbook and take the single check and not the whole checkbook with you.

Five: Smartphone/Tablet/Laptop not Password Protected

These days, our cell phone, smartphone, tablet or laptop devices are like an extension of our bodies. We are at a loss if we don't have them with us. According to the Identity Theft Resource Center, 62% of smartphone users don't have a password on their home screen. Thus giving free access to anyone that might steal their phone to their personal information.

Another mistake is putting personal information like passwords, PIN codes, credit card numbers, etc. in the Contacts or Notes applications. These store this information unsecure and in plain text. It is important that you password protect your mobile devices.

I would also recommend using a "strong password" for your home screen. That is a password that is over 8 characters long, uses both upper-case and lower-case letters as well as special characters. Your password shouldn't be something that would be easy to guess.

I also would recommend the use of a secure application for storing passwords and personal information instead of using the Notes and Contacts applications.

Six: Passport

Your passport is another potential "goldmine" for an identity thief; especially if they have in mind to commit international crime using your identity.

Of course, if you are traveling, you can't just leave your passport at home. However, you can make a copy of it and leave the original locked away in a hotel safe.

When traveling, carry with you the local address and phone number of your embassy. In the event your passport is stolen, you should contact them.

Seven: Account Statements

Another thing some people do is to carry around their account statements with them. This could be their bank statement, credit card statement, home mortgage, etc.

That information in the hand of an identity thief could allow them to open up additional accounts in your name. Also if the identity thief has enough of your personal information, they could hack into credit reporting service sites or healthcare sites by using the information they have and guessing at the other information.

Do yourself a favor and leave your account statements stored securely at your home.

There you have it “7 things to leave at home”. Of course this is not an exhaustive list. The idea is to use good judgment and to be proactive in protecting your identity.

By doing that, you’ll gain the peace of mind knowing that you are doing what you can to protect your identity.

Resources

Credit Reporting Agencies

- Equifax: 1-800-525-6285 www.equifax.com
- Experian: 1-888-397-3742 www.experian.com
- TransUnion: 1-800-680-7289 www.transunion.com

Credit Monitoring

- Free annual credit report: www.annualcreditreport.com
- Credit Monitoring Service:
<http://truthonidtheft.com/id-theft-protection/>

Government Agencies

- Federal Trade Commission: www.ftc.gov
- FTC Online Complaint:
<https://www.ftccomplaintassistant.gov/>
- Internet Crime Complaint Center (IC3): www.ic3.gov
- Social Security Administration: www.socialsecurity.gov/
- Federal Bureau of Investigation (FBI): www.fbi.gov/

Miscellaneous

- Identity Theft Information: www.TruthOnIDTheft.com
- Identity Theft Protection Products:
www.TruthOnIDTheft.com/id-theft-protection-products/