Identity Theft is a form of fraud or cheating of another person’s identity in which someone pretends to be someone else by assuming that person’s identity, typically in order to access resources or obtain credit and other benefits in that person’s name. The victim of identity theft can suffer adverse consequences if he or she is held accountable for the perpetrator’s actions. Organizations and individuals who are duped or defrauded by the identity thief can also suffer adverse consequences and losses, and to that extent are also victims.

Identity theft continues to increase every year and has impacted millions of Americans.

Consider these sobering statistics:

- Identity theft continues to be the fastest growing crimes in the world
- 11.1 million adults in the US alone were victims of identity theft in 2009
- The total fraud amount was $54 billion
- The average victim spent 21 hours and $373 out of pocket resolving the crime
- 4.8% of the population was a victim of identity fraud in 2009
- 13% of identity fraud crimes were committed by someone the victim knew

Identity theft usually takes the form of five major categories:

- Business/commercial identity theft (using another’s business name to obtain credit)
- Criminal identity theft (posing as another person when apprehended for a crime)
- Financial identity theft (using another’s identity to obtain credit, goods and services)
- Identity cloning (using another’s information to assume his or her identity in daily life)
- Medical identity theft (using another’s identity to obtain medical care or drugs)
How Identity thieves get your personal information:

- They steal wallets and purses containing your identification and credit/bank cards.
- They steal your mail (bank and credit card statements, pre-approved credit offers, telephone calling cards, tax information, etc.)
- They complete a “change of address form” to divert your mail to another location.
- They practice “dumpster diving” (rummaging through your trash for personal data).
- They fraudulently pose as a landlord, employer or someone else who may have a legitimate need for – and a legal right to – your credit report data.
- They find personal information in your home.
- They obtain your business or personal information at your work.
- They use personal information you share on the Internet.
- They steal or access your Smart Phone

How identity thieves use your personal information:

- They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take several months before you realize there is a problem.
- They open a new credit card account, using your name date of birth and SSN. When they use the credit card and don’t pay the bills, the delinquent account is reported on your credit report.
- They establish phone or wireless service in your name and run up huge bills.
- They open a bank account in your name and write bad checks on that account.
- They counterfeit checks or debit cards, and drain your bank account.
- They buy cars by taking out auto loans in your name.

What can you do to help prevent becoming a victim?

*Buy a cross-cut type shredder* (you can purchase cross-cut type shredder very cost effectively for approximately $60 - $70.) Shred all your important papers and especially pre-approved credit applications received in your name and other financial information that provides access to your private information. Don’t forget to shred your credit card receipts.
Minimizing Identity Theft

Be careful of “Dumpster Diving.” Make sure that you do not throw anything away that someone could use to become you. Anything with your identifiers must be shredded (cross-cut) before throwing away.

Be careful at ATM’s and using Phone Cards. “Shoulder Surfers” can get your “Pin Number” and get access to your accounts.

Get all of your checks delivered to your bank - not to your home address.

Do not put checks in the mail from your home mailbox. Drop them off at a U.S. Mailbox or the U.S. Post Office. Mail theft is common. It’s easy to change the name of the recipient on the check with an acid wash.

When you order new credit cards in the mail, or your previous ones have expired, watch the calendar to make sure that you get the card within the appropriate time. If it is not received by a certain date, call the credit card grantor immediately and find out if the card was sent. Find out if a change of address was filed if you don’t receive the card or a billing statement.

Cancel all credit cards that you do not use or have not used in 6 months. Thieves use these very easily - open credit is a prime target.

Memorize social security numbers and passwords.

Put passwords on all your accounts and do not use your mother’s maiden name. This can be easily determined using public records Make up a fictitious word.

Get a post office box or a locked mailbox, if you possibly can.

Ask all financial institutions, doctors’ offices, etc., what they do with your private information and make sure that they shred it and protect your information. Tell them why.

Empty your wallet of all extra credit cards and social security numbers, etc. Do not carry any identifiers you do not need. Don’t carry your birth certificate, social security card, or passport, unless necessary.

When a person calls you at home or at work, and you do not know this person, never give out any of your personal information. If they tell you they are a credit grantor of yours call them back at the number that you know is the true number, and ask for that party to discuss personal information. Provide only information that you believe is absolutely necessary.
**Minimizing Identity Theft**

**NEVER put your social security number on your checks or your credit receipts.** If a business requests your social security number, give them an alternate number and tell them why. They do not need that to identify you. If a government agency requests your social security number, there must be a privacy notice accompanying the request.

**Get credit cards and business cards with your picture on them.**

**Do not put your credit card account number on the Internet** (unless it is encrypted on a secured site.) Don’t put account numbers on the outside of envelopes, or on your checks.

**When you are asked to identify yourself at schools, employers, or any other kind of institutional identification,** ask to have an alternative to your social security number. Unfortunately, your health insurance carrier often uses your social security number as your identification number. Try to change that if you can.

**In conjunction with a credit card sale do not put your address, telephone number, or driver’s license number on the statement.**

**Sign up for an Identity Theft Protection service**

**Monitor all your bank statements from every credit card every month.** Check to see if there is anything that you do not recognize and call the credit grantor to verify that it is truly yours.

**Order your credit report at least twice a year** (I have enclosed the addresses for you on the sample letter.) Review it carefully. If you see anything that appears fraudulent, immediately put a fraud alert on your reports by calling the numbers below.

**Do not put your telephone number on your checks.**

**Immediately correct all mistakes on your credit reports in writing.** Send those letters Return Receipt Requested, and identify the problems item by item with a copy of the credit report back to the credit reporting agency. You should hear from them within 30 days.

**NEVER put your social security number on your checks or your credit receipts.**

**Do not put checks in the mail from your home mailbox.**
Watch Your Phone!

Attacks on Google’s Android smartphones quadrupled, and smartphones running Java-based applications jumped 45%. The trend is projected to get even worse as prices for smartphones continue to decline and more and more people buy them. Now that smartphones double as wallets and bank accounts -- allowing users to manage their finances, transfer money, make payments, deposit checks and swipe their phones as credit cards -- they are very lucrative scores for thieves. And with 30% of phone subscribers owning iPhones, BlackBerrys and Droids, there are a lot of people at risk.

Here’s some steps you can take to help prevent a thief from accessing your smartphone:

- Set up a password and keep your phone locked when you aren’t using it
- Avoid using an unsecured Wi-Fi connection – especially when accessing sensitive info
- Never download anything from an untrusted source – unless you want a virus
- Delete everything off your old smartphone before you get rid of it

The majority of smartphones on the market have a feature that lets you wipe your phone remotely. That way your personal information can be erased even if it is lost or stolen.

You can also spend a little money and get anti-virus protection for your phone.

New Websites:

- [www.identitytheft.info](http://www.identitytheft.info)
- [www.identitylabs.com](http://www.identitylabs.com)
- [www.identitytheft.org](http://www.identitytheft.org)
- [www.ftc.gov](http://www.ftc.gov)