

# **Identity Theft – It Can Happen to You!**

**By Barbara R. Linker**

## **What is Identity Theft?**

Identity Theft is what happens when someone uses your personal information to commit fraud in your name. Identity thieves can do a lot of damage resulting in devastation to the victim. They can go on spending sprees using your credit card, open a new credit card account using your name and Social Security number, get cell phone service in your name with your credit history, and even get arrested and give your name to the police. The victim can lose out on job opportunities, loans for education, housing or cars, and they may even be arrested for crimes they didn't commit.

Identity Theft can also occur in the business environment where employees steal information, or bribe another employee for information, con information from other employees, hack into computer records, or simply take information from the trash. Identity Theft can happen to you personally by having your purse or wallet lost or stolen.

How often do you receive “phishing scams” in your email? Phishing is when someone sends an e-mail to you and claims to be a legitimate company that attempts to scam you into surrendering private information that they'll use for identity theft. The email will contain a link to visit a web site where you would be asked to update your personal information, such as passwords, credit cards, social security number, and bank account numbers. Of course the web site is bogus and set up only to steal your information.

Telemarketers do what is called “pre-texting”. Pretexting is when someone obtains your personal information under false pretenses and it is against the law. Your information will be sold to people who may use it to get credit in your name, steal your assets, or to investigate or sue you.

“Skimming” is another way thieves get your information. Skimming is a hi-tech method where thieves capture your personal or account information from your credit card, driver's license, or passport. A “skimmer” is an electronic device used to capture this information and can be purchased online for under \$50.00. When your card is swiped, the skimmer captures your information from the magnetic strip on the card and stores it on the device itself, or on a device attached to the skimmer.

Other ways your information is obtained is by someone abusing your credit report or tampering with your mail. Did you know that identity thieves will fill out a change of address form at the post office so that your bills and other personal information will be sent to them?

What do thieves do once they have your information?

- Call your credit card company and change your address
- Open credit cards in your name and not pay bill
- Apply for phone and wireless services and rack up the charges
- Open a bank account and write bad checks
- Drain your bank account using counterfeit checks, EFTs, credit/debit cards
- File Bankruptcy in your name to avoid paying bills
- Get a Drivers License in your name with their picture on it
- Get a job or file fraudulent tax returns in your name
- Give your name to police during an arrest, don't show up in court, and there is a warrant out for your arrest.

It may take some time for you to realize you're a victim of identity theft, and the damage can be devastating, but you can take some practical steps to minimize your risk and reduce the damage.

To determine if you are a possible victim, check your credit report for accounts open in your name that you didn't initiate, and check your bank accounts for charges and withdrawals that you didn't make. Other clues to being a possible victim of identity theft are; being denied credit for no apparent reason, getting calls from debt collectors or companies about merchandise you didn't purchase, or missing bills in the mail that you normally get.

### **What to do if you are a victim of Identity Theft**

There are four things you need to do if you are a victim of identity theft. You need to:

1. Place a "fraud alert" on your credit reports
2. Close all accounts that are affected
3. File a police report
4. File a complaint with the FTC.

A fraud alert on your credit report will prevent accounts from being open in your name. When you put a fraud alert on your credit report you are entitled to a free credit report for your review. The 3 major Credit Reporting Agencies are; Equifax (1-800-525-6285), Experian (1-888-397-3742), and TransUnion (1-800-680-7289). Review all three credit reports and report all fraudulent and inaccurate information immediately.

Close all accounts that are affected by calling the "Security Fraud Department" at each establishment. It is very important that everything you do is documented! Follow up all your phone conversations in writing, and include copies of any supporting documents. Do not send originals! Send all correspondence by Certified Mail/Return Receipt, and keep a record of what companies receive and when. Keep a file of all your correspondence and enclosures.

File a police report and get a copy of it, or at least get the report number. Not all police stations will take a report for identity theft, and if you find you are getting the runaround, try another law enforcement agency like the Sheriff's Office or State Police.

File a complaint with the Federal Trade Commission. This will help law enforcement across the country track down identity thieves and stop them. The FTC can also refer victim's complaints to other government agencies and companies for further action. The FTC can be reached by phone at: 1-877-438-4338 or on the web at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

### **How to protect yourself from Identity Theft**

By making your personal information hard to get, you can reduce your risk of being victim. Four things you need to know to protect yourself from identity theft are:

1. Safeguard your personal information
2. Use the shredder
3. Protect your social security number
4. Protect your computer.

Safeguard your personal information in a secure place in your home, especially if you have roommates, employ outside help, or are having work done in your home.

The shredder is your friend! Those pre-approved credit applications you get in the mail all the time? Shred them! Better yet, you can call 1-888-5-OPTOUT. Also shred credit card receipts

when you no longer need them. Insurance forms should also be shredded because they contain personal information such as SSN and salary information. Physician statements and bills should be shredded because the information can be used to take your identity and before you know it, someone is receiving medical treatment or obtaining drugs in your name and using your medical insurance.

Protect your Social Security number by keeping it in a safe, secure place, and never carry it in your wallet. If your SSN is being used as an identifying number, request that some other identifying number be used. If someone asks you for your SSN, ask them questions like “Why do you need it?”, “How will it be used?”, “How do you protect it from being stolen?” and “What will happen if I don’t give it to you?”

In this day and age it is critical to protect your computer from any chance of personal information being compromised. If you are a broadband user, turn off the computer when not in use. Create Backups of your important files on a regular basis, preferably by automatically having a backup program run at a time when your computer is not being used (like when you’re sleeping). Turn off HTML e-mail. HTML email can contain commands to be executed by your email client, so when you read HTML email you are allowing the sender to give commands to your computer. Some of these commands can be used maliciously to exploit common security holes which can expose you to spam, computer viruses, and worms. Delete spam without reading it and never click on links unless you are sure of them.

In addition, you also need to protect against intrusions and infections by updating your virus protection software on a regular basis. Take precautions to avoid “spyware” which can capture your passwords or other information as you type it into your keyboard. Use a firewall, particularly if you have a Cable, DSL, or T-1 connection that leaves your computer connected to the Internet 24 hours a day. Using a firewall will stop uninvited access to your computer.

When processing transactions online, check and make sure that you are using a “secure browser”. You can check this by looking for the “lock” icon on the browser’s status bar, or by checking the web address line for https://

Remember that criminals are out there, looking for identity information to steal. They like identity theft because it can be such a so-called “easy” crime. They do their best work when no one is paying attention and information is easy to get, because they think the damage will go undetected.

The FTC is urging you to:

- DETER identity thieves by safeguarding your information
- DETECT suspicious activity by routinely monitoring your financial accounts and billing statements
- DEFEND against identity theft as soon as you suspect a problem

ID-Theft document downloads and links can be found at <http://www.linker-mobile-notary.com/ID-Theft.htm>