

How Important Is Your Personal Identity?

Identity Theft. Most likely, you have heard the phrase and hope it will never happen to you. Just the thought of having your personal identifying information stolen by someone, who will use your good name and credit history, to gain access to your financial accounts with the intent to commit fraud or a theft is extremely unnerving.

Identity theft is a serious crime. In fact, it's the fastest growing crime in our nation. But how many of us even heard of identity theft a decade ago? However, these days, it's very common and it can happen to you. More than ten million people are victimized each year. If you haven't been a victim of identity theft, consider yourself fortunate because you probably know of someone who has been. Maybe you have heard about the costs and the hours of cleaning up the mess the thieves have made of your credit record.

What are some of the common ways identity theft happens? Skilled identity thieves use a variety of methods to steal your personal identity, including:

- ⇒ Dumpster Diving – They rummage through trash looking for discarded bills, financial or credit card statements, receipts from purchases or any other documents with your personal information on them.
- ⇒ Stealing – They steal wallets, purses, mail; especially bank and credit card statements, pre-application credit card offers, new checks and tax information. These documents may contain such personal information as: your name and birth date, social security number, credit/debit card numbers, etc. They may also steal personnel records from their employer or use someone who has computer access to personal information from a variety of venues.
- ⇒ Online “Phishing” – They pretend to be financial institutions or companies and send you spam mail or pop-up messages, which may look very realistic, in order to get you to respond with your personal information.
- ⇒ Changing Your Address – They divert your billing statements to another location by completing a “change of address” form or by simply calling the company requesting the change.
- ⇒ Skimming – They steal credit/debit card numbers by using a special storage device when processing your card. Your card numbers can then be used unlawfully by someone who has had legitimate access to them.

This list is not exhaustive because identity thieves are thinking of new and inventive ways to unlawfully use your information every day.

So the question you may be asking is, “Can I prevent an identity theft?” As is true with any crime, you cannot completely control whether you will become a victim or not. Who is vulnerable? To some degree, all of us are. The good news is you can minimize the risk of becoming a victim by managing your personal information cautiously.

The Federal Trade Commission has given us a concise and practical message about identity theft: **Deter, Detect, Defend**. Most of these recommendations are common sense precautions you may be already practicing. Here are some things you can do to protect yourself:

DETER identity thieves by safeguarding your personal information.

- ✓ Shred all financial documents, receipts or paperwork with personal information before you discard them.
- ✓ Deposit your outgoing mail at a Post Office or a blue U.S. Postal Service collection box, or give it directly to your letter carrier.
- ✓ Report lost or stolen credit/debit cards to the issuing bank immediately. Additionally, don't leave your transaction receipts behind. Take them with you.
- ✓ Protect your Social Security number. Don't carry your Social Security card with you or write it on a check. Memorize it. Give it out only if absolutely necessary (on an income tax return for example) or ask to use another identifier.
- ✓ Don't give out personal information on the phone, through the mail, or over the internet unless you initiated the contact and know the person you are dealing with.
- ✓ Never click on links sent in unsolicited e-mails. Instead, type in a web address you know. Use firewalls, anti-spy ware and virus software to protect your home computer; keep them up-to-date.
- ✓ While using your computer, don't use obvious passwords like your birth date, your mother's maiden name, or the last four digits of your Social Security number. Use a combination of numbers and letters.
- ✓ Lastly, keep your personal information in a secure place at home, especially if you employ outside help or are having work done in your home.

DETECT suspicious activity by routinely monitoring your financial accounts and billing statements. Be alert to signs requiring immediate attention:

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Phone calls or letters about purchases you did not make

Inspect:

- ⇒ Your financial statements – Check your bank, credit card and similar statements regularly. Call your bank or credit card companies if you don't receive your bill.
- ⇒ Your credit report – Credit reports contain important information about you, including what accounts you have and your bill paying history. The law requires the major nationwide consumer reporting companies to give you a free copy of your credit report each year if you ask for it. You can do this on-line by visiting: www.AnnualCreditReport.com or www.FreeCreditReport.com. You can also call 1-877-322-8228 to order your credit report.

DEFEND against Identity Theft as soon as you suspect it.

- ✓ Place a “Fraud Alert” on your credit reports and review the reports carefully. The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. Also, placing a fraud alert entitles you to free copies of your credit reports. When examining the credit reports, look for inquiries from companies you haven’t contacted, accounts you did not open, and debts on your accounts you can’t explain. To place a fraud alert contact one of the credit reporting bureaus:
 - Equifax Credit Information Services, Inc
800-525-6285
 - Experian
800-397-3742
 - TransUnion
800-888-4213

- ✓ **Close Accounts.** Close any accounts that have been tampered with or established fraudulently.
 - * Call the security or fraud departments of each company where an account was opened or changed without your approval. You may want to follow up in writing, with copies of supporting documents.
 - * Use the ID Theft Affidavit at www.ftc.gov/idtheft to support your written statement.
 - * Ask for verification that the disputed account has been closed and the fraudulent debts have been discharged.
 - * Keep copies of the documents and records of your conversations about the incident.

- ✓ **File a police report.** File a report with your police department to help you with creditors who may want proof of the crime and for documentation purposes.

- ✓ **Report the ID theft to the Federal Trade Commission.** Your report helps law enforcement officials across the country in identity theft investigations. You can report Online: www.ftc.gov/idtheft or by phone 1-877-ID-THEFT (438-4338)

Lastly, there are many resources available through the Federal Trade Commission to learn more about identity theft and how to deter, detect and defend against it. By having an understanding of how this crime occurs, and minimizing the risks by managing our personal information carefully, we can help protect ourselves from becoming victims.