# IDENTITY THEFT: HOW TO PROTECT YOURSELF

## What Is Identity Theft?

Identity theft can take many forms but all of them involve stealing someone's identity for financial gain (to open a new bank or credit card account), nonfinancial gain (to open a cell phone or other utility account), or to avoid a legal sanction (taking someone else's identity to avoid a speeding ticket).

## How Are Identities Stolen?

There are several types of information that an identity thief might want. The information includes not just your name but also your Social Security Number, driver's license number, account numbers, other ID numbers, your address, passwords, and other personal information. They can steal this information:

- From an unsecured mailbox
- From your trash or public dumpsters
- From your purse or wallet
- By phishing – Sending e-mail to get you to respond with personal information
- By pharming – Redirecting a web site's traffic to another, bogus site to collect personal information
- By phone, when the caller pretends to ask for personal information for a survey or a charity
- Online in a phony employment web site designed to gather personal information
- In data breaches, when hackers break into an organization's web site, personal information is accidentally posted to the web, or an employee steals or loses data on a laptop or data storage device.

## How Can You Avoid Identity Theft?

- Don't put outgoing mail in unsecured mailboxes.
- Watch your mail. If a bill or statement doesn't arrive on time, check it out.
- Be sure no one is listening if you give out personal information on the phone.
- Don't put personal information on a portable storage device or laptop that you carry with you.
- Check your credit card statements and bank records for unfamiliar transactions.
- Don't have new checks mailed to an unsecured mail box.
- Don't give out personal information via e-mail or the phone unless you initiated the contact or know who you're communicating with.
- Buy a shredder and shred all documents with personal information or account numbers, including pre-approved credit offers.
- Choose passwords and Personal Identification Numbers (PINs) that aren't based on easily available information such as your birth date, Social Security Number, or phone number.
- Keep your personal information in a secure place at home and at work.
- Check your credit report. Look for unfamiliar transactions. If you find any inaccurate information, report it in writing to the credit bureau immediately.
- Don't put personally identifying information on a MySpace or Facebook page or a personal web site.
- Think before giving your Social Security Number – at school and elsewhere.

# IDENTITY THEFT: HOW TO PROTECT YOURSELF

## What Should You Do If Your Identity Is Stolen?

- Put a fraud alert on your credit reports and review your credit reports. Contact any one of the credit bureaus to put a fraud alert on your file at all three credit bureaus. The initial fraud alert stays on your credit report for at least 90 days. An extended alert stays on your credit report for seven years. The alert means a business must verify your identity before extending credit. It protects you but could slow things down when you apply for credit.
- Close accounts that have been tampered with. Call the security or fraud department of each company. Follow up in writing and send copies (NOT originals) of supporting documents. Send letters by certified mail so you can document what the company received and when.
- If there are fraudulent charges on your accounts, or the thief opened new accounts, ask the company for forms to dispute the charges or write a letter. Send the letter to the address for billing inquiries. Once the dispute is resolved, ask the company for a letter stating that.
- File a complaint with the Federal Trade Commission. You can file using the online ID Theft Complaint form at www.ftc.gov or call the FTC Identity Theft Hotline at 1.877.ID.THEFT.
- File a report with your local police or the police in the community where the identity theft took place. Get a copy of the report or at least the number. Take a copy of your ID Theft Complaint form and supporting documents with you to the police. Ask the officer to attach or incorporate the complaint in the police report.

## To Request a Copy of Your Credit Report:

Access your free annual credit report at http://www.annualcreditreport.com.
(You will ultimately pay for your credit report from any other web site.)

Georgia residents also have a right to two free credit reports a year. You can request those at:

| Equifax | Experian | Trans Union |
|---|---|---|
| 1-800-685-1111 | 1-888-397-3742 | 1-800-888-4213 |
| www.equifax.com | www.experian.com/freestate | www.transunion.com |

## To Freeze Your Credit

You may now contact a credit bureau to freeze your credit so no one (including you) can open a new credit account in your name. Georgia law limits the credit bureaus' charge to you to $3 (at each of the three credit bureaus). For another $3, you can unfreeze your credit for quick, on-the-spot credit applications – for a store credit card, for example. There's no charge to freeze your credit if you're a victim of identity theft or over age 65. Check the credit bureaus' websites to learn how to freeze your credit.

## To Place a Fraud Alert:

Call any one of the three credit bureaus at:

- Equifax: 1-800-766-0008
- Experian: 1-888-397-3742
- Trans Union: 1-800-680-7289