Identity Theft

Learn how to protect yourself from the fraudulent acquisition and use of your private identifying information for financial gain.

When in Public:

- Leave your Social Security card at home. You will only need it in public to verify your right to obtain employment, so there is no reason to store it in your wallet.
- Limit what you carry. When you go out, take only the identification, credit, and debit cards you need.
- Lock your wallet or purse in a safe place at work.
- Before you share information at your workplace, a business, your child's school, or a doctor's office, ask why they need it, how they will safeguard it, and the consequences of not sharing.
- Make a list of all 1-800 customer service numbers located on the back of your bank cards and credit cards. Keep these numbers in your phone and a safe place at home. In the event your cards are lost or stolen, this will allow you to stop transactions as quickly as possible. Do not list any account information. You can verify yourself as the account holder when you call.
- Do not send your personal information or make transactions using a publicly shared wireless network. These networks are most commonly located in coffee shops, libraries, airports, and hotels. They may not encrypt the data you send, making it susceptible to hackers.
- Turn the Wi-Fi off on your smartphone when it's not in use. This will keep hackers from picking up your signal and trying to hack into your network.

When at Home:

- Lock your financial documents and records in a safe place at home.

- Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don’t need them any longer.
- Make sure you know who is getting your personal or financial information. Don’t give out personal information on the phone, through the mail, or over the internet unless you’ve initiated the contact or know with whom you are dealing.
- If a company that claims to have an account with you sends an email asking for personal information, do not click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service.
- When you order new checks, don’t have them mailed to your home. Ask your bank if they can send them to your branch for pickup.
- Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often.
- Never store sensitive information in the hard drive of your computer where it is exposed to hackers. Keep all of your electronic personal information (such as tax returns and medical information) secured on an external storage device. Keep this device securely locked away in your home when it's not in use.
- If you post too much personal information about yourself on social media, an identity thief can use it to answer "challenge" questions on your accounts to gain access.
- Take outgoing mail to Post Office collection boxes or the Post Office. Promptly remove mail that arrives in your mailbox.
- If you are not home for several days, request a vacation hold on your mail.

If you are a Victim:

Step 1:

Stop all transactions immediately. Call all of the financial institutions you bank with or have credit with and have them stop anyone from making further purchases.

Step 2:

Contact each of the three credit reporting agencies (see reverse) and place a fraud alert on your credit report. You can even freeze your credit report. This will stop any new activity but understand; you will not be able to obtain new credit until you unfreeze it.

Step 3:

Change all online passwords to accounts, email addresses, and any online stores.

Step 4:

Contact your local law enforcement agency and file a police report. Be sure you have copies of supporting documents showing any unauthorized transactions to accompany the report.

Step 5:

Request all Affidavit materials for disputing unauthorized charges from each financial institution where there was a transaction. Complete and return the materials along with the case numbers of any police reports.

Step 6:

Be sure to dispute any negative entries on your credit report that were a result of unauthorized charges. Provide supporting documentation as requested.

Step 7:

Continue to be diligent about monitoring your credit report, bank statements, and credit card statements for any additional activity.