

Identity Theft

Identity theft is a serious crime. People whose identities have been stolen can spend months or years — and thousands of dollars — cleaning up the mess the thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans for education, housing, cars, or even be arrested for crimes they didn't commit.

At Walden Federal, we're committed to protecting your privacy and security. We will never initiate a request for sensitive information from you via email (ie., Social Security Number, Personal ID, Password, PIN or account number). We strongly recommend that you do not share your Personal ID, Password, PIN or account number with anyone, and never provide this information in response to an e-mail ("phishing"). Please see our page on "phishing" for more details on recent e-mail fraud.

Despite your best efforts to manage the flow of your personal information or to keep it to yourself, skilled identity thieves may use a variety of methods — low- and hi-tech — to gain access to your data. Here are some of the ways imposters can get your personal information and take over your identity.

How identity thieves get your personal information:

- They steal wallets and purses containing your identification and credit and bank cards.
- They steal your mail, including your bank and credit card statements, pre-approved credit offers, new checks, and tax information.
- They complete a "change of address form" to divert your mail to another location.
- They rummage through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving."
- They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for, and legal right to, the information.
- They find personal information in your home.
- They use personal information you share on the Internet.
- They scam you, often through email, by posing as legitimate companies or government agencies you do business with.
- They get your information from the workplace in a practice known as "business record theft" by: stealing files out of offices where you're a customer, employee, patient or student; bribing an employee who has access to your files; or "hacking" into electronic files.

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 some time before you realize there's 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.
- They open a bank account in your name and write bad checks on that account.

- They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- They counterfeit checks or debit cards, and drain your bank account.
- They buy cars by taking out auto loans in your name.
- They give your name to the police during an arrest. If they're released from police custody, but don't show up for their court date, an arrest warrant is issued in your name.

You can't totally protect yourself from identity theft, but you can significantly reduce your risk by carefully safeguarding your personal information.

What you can do

- Ensure that your credit information is accurate by ordering a copy of your credit report from the 3 main credit bureaus.
- Avoid passwords on accounts that are easily available such as birth dates, mother's maiden name, etc.
- Secure personal information in your home so that it's not easily accessible to cleaning help, repairpersons, etc.
- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers (ISPs) and even government agencies to get you to reveal your SSN, mother's maiden name, account numbers and other identifying information.
- Guard your mail and trash from theft. Shred or tear account statements, charge receipts, credit offers, etc. before discarding.

Protect your computer information too

- Update your virus protection software regularly, or when a new virus alert is announced.
- Do not download files sent to you by strangers or click on hyperlinks from people you don't know.
- Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL or T-1, which leaves your computer connected to the Internet 24 hours a day.
- Use a secure browser — software that encrypts or scrambles information you send over the Internet — to guard the security of your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer.
- Before you dispose of a computer, delete personal information. Deleting files using the keyboard or mouse commands may not be enough because the files may stay on the computer's hard drive, where they may be easily retrieved.

What to do if you are a victim of identity theft

Immediately report the fraudulent activity to credit bureaus, banks, credit card companies, etc. If appropriate, report the fraud to local law enforcement agencies.

Contact the Federal Trade Commission (FTC) at 1-877-IDTHEFT or visit their web site at www.ftc.gov/idtheft for further details and key contact information and sample forms.