T-I fcu
Temple-Inland Federal Credit Union

Identity Theft

Identity theft describes various means by which criminals are able to obtain personal and financial information about people. This information can then be used for fraud activity by stealing from a person's account, counterfeiting credit cards, or establishing credit using the victim's identity.

The theft of personal information may include Social Security Numbers (SSN), bank account or credit card account numbers, user names and passwords used in electronic activity, and other types of personal information, all of which can be used for fraudulent activity.

* Common means in which criminals attempt to steal identifying information include:

Paper and Card Theft: Stealing a purse or billfold or "dumpster diving" to look through trash for copies of account statements and other paper information.

Skimming: This is the use of hand-held devices to capture the magnetic information strip from a credit or debit card. This is most often done at a point of purchase where a person gives a credit card to a clerk or waiter.

Insider Theft: Someone inside an organization (an employee) steals and sells customer information.

Phishing: Phishing usually involves fraudulent e-mails and bogus websites that trick people into revealing personal and account information.

Pretexting: This is an attempt by telephone contact to trick people into providing personal and account information. The criminal pretends to be from a financial institution and uses all sorts of explanations for why the information is needed.

Pharming: This is when a criminal hacks into the computer system of a business and redirects links on the company's website, such as a financial institution's link to its home banking service.

Spyware: This involves the introduction of a virus or other software onto an individual's computer that allows a criminal to capture keystrokes such as user name and password when logging onto an online account, or credit card information when making an online purchase.

These are some general tips for avoiding Identity Theft.

- Never dispose of anything with sensitive personal information in the regular trash or in a public trash container.
- Use a paper shredder to dispose of sensitive paper, such as bank and credit card statements, before putting them in the trash.
- If you receive an e-mail or pop-up message asking for personal or account information, do not reply and do not follow any link contained in the message.
- Never open an e-mail attachment unless you are sure of the sender and what is in the attachment. This is one way viruses can be put on your computer. A safe approach is to delete e-mails from unknown sources without opening them.
- Be sure your computer is equipped with current antivirus software and the latest security patches.
- Set your Internet browser to prompt you if a website tries to install software.
- Avoid sending personal and financial information over the Internet if you are not sure of the website and that the page is secure.
- Avoid sending personal and financial information via e-mail to avoid your information being intercepted by a criminal.
- Carefully review your credit card and other account statements immediately upon receiving them.
- Review your credit reports regularly.

If you should become a victim of Identity Theft there are four primary steps that you should take.

1. Contact all three national reporting agencies to place a fraud alert on your credit reports. You should start with a phone call to each and follow up with a letter or email.

Experian
Fraud # 1-888-397-3742
P.O. Box 2104
Allen, TX 75013-2104
www.experian.com

Equifax
Fraud # 1-888-766-0008
Equifax Credit Information Services, Inc
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Transunion Corporation
Fraud # 1-800-680-7289
TransUnion LLC
Consumer Disclosure Center
P.O. Box 1000
Chester, PA 19022
www.transunion.com

2. Alert all financial institution(s). They will close your account(s), open new ones, and order new checks and debit cards.

3. File a police report at your local police department. Keep a copy for your records.

4. File a claim with the FTC at 1-877-ID-THEFT (1-877-438-4338) or www.FTC.GOV/IDTHEFT

What You Can Do to Help Protect Your Privacy

Temple-Inland Federal Credit Union is committed to protecting the privacy of its members. Members can help by following these simple guidelines:

Protect your account numbers, card Numbers, and PINs or passwords.

Use caution when disclosing your account number, social security number, etc. to other persons. If someone calls you and explains the call is on behalf of the credit union and asks for your account number, you should beware. Official credit union staff will have access to your information and will not need to ask for it.

Keep your information with us current. It is important that we have current information on how to reach you so if your address or phone number changes, please let us know. If we detect potentially fraudulent or unauthorized activity of your account, we will attempt to contact you immediately.