

About Identity Theft

Identity theft can be best described as the misuse of personal information for financial gain. The most common types of identity theft complaints reported are;

- Credit Card Fraud
- Unauthorized Phone or Utility Services Fraud
- Bank Fraud
- Fraudulent Loans Fraud
- Government Document or Benefits Fraud.

Criminals usually gain access to a victim's personal information from stolen wallets or mail and also through hacked emails and computers. Below are a few tips useful in preventing Identity Theft.

1. Don't provide your social security number or personal credit information to anyone over the phone unless you are the one that initiated the call and are familiar with the business.
2. Don't provide any personal information via text message or on social networking sites.
3. Tear up or shred all credit card receipts, bank statements, credit card offers, and any unused cards before throwing them in the trash or recycling them.
4. Protect your bank and credit card Personal Identification Numbers (PINs).
5. Don't use a birth date or Social Security Number as a password.
6. Remove yourself from direct mailing lists at the three credit reporting bureaus.
7. Keep a list of all of your credit cards, account numbers, expiration dates, and customer service or fraud department telephone numbers in a secure place away from the cards for easy access if you need them.
8. Never keep your Social Security Card in your wallet and don't print your Social Security number on your checks.
9. Check through your credit card statements carefully and immediately report any unusual activity.
10. Be cautious when entering a login ID and PIN for all online account access when in public and also when using wireless hotspots for online account access.
11. Make sure you are on a secure website by ensuring your browser's padlock key is active. Also look for an "s" after the "http" to be sure the website is secured.
12. Set up text or email alerts from your bank for certain types of transactions. Call bank for details.
13. Sign up for online banking to reduce the likelihood of paper statements being stolen.
14. Make sure the virus protection software on your computer is active and up to date.
15. Use the passcode on your smart phone or other devices. It will be harder for people to access your information if your phone is lost or stolen.
16. If you think someone has learned your login ID and password, notify us and we can help you change your passwords to your accounts that have been compromised.

Credit Reporting Agencies

Equifax - www.equifax.com

To order your report, call: 1-800-685-1111 or write: P.O. Box 740241, Atlanta, GA 30374-0241

To report fraud, call: 1-800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241

Experian - www.experian.com

To order your report, call: 1-888-EXPERIAN (397-3742) or write: P.O. Box 2104, Allen, TX 75013

To report fraud, call: 1-888-EXPERIAN (397-3742) and write: P.O. Box 9532, Allen, TX 75013

Trans Union - www.tuc.com

To order your report, call: 1-800-916-8800 or write: P.O. Box 1000, Chester, PA 19022

To report fraud, call: 1-800-680-7289 and write: Fraud Victim Assistance Division

P.O. Box 6790, Fullerton, CA 92834

If you've been a victim of identity theft, file your complaint with the Federal Trade Commission:

Identity Theft Hotline Toll-Free 1-877-438-4338

TDD 202-326-2502

By mail: Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue
Washington, DC 20580

Online www.consumer.gov/idtheft