



WHAT IS IDENTITY THEFT?

What is Identity Theft?

Identity theft takes place when someone steals your personal information (such as your name, social security or bank account number) to commit fraud. These thieves use the information to repeatedly commit fraud in an attempt to duplicate your identity. Identity theft can have a negative effect on your credit and create a financial hassle for you. Take action to minimize the chances of becoming a victim of identity theft.

Ways People can steal your Identity:

1. Lost or stolen information like Social Security Cards, checkbooks, credit cards or your mail can provide criminals with enough data to commit fraud.
2. Onlookers at the ATM or in stores may get your PIN while you are using your debit card. (First United Bank's Check Card can be used for signature transactions by simply selecting the "Credit" function when using the credit/debit card terminals at retail store locations.)
3. Inside jobs are also a threat to your security. An employee of a business such as a doctor's office or financial services company may illegally access personal information and sell it to identity thieves.
4. The Internet creates a place that criminals collect critical personal information. They use the Internet to look for personal pages that contain information like genealogical data with your mother's maiden name that can be used to set up a credit card account or possibly access existing accounts.
5. Phishing is an attempt to steal confidential information from consumers through the use of "pop-ups" or emails. These emails have Internet links to deceive you into disclosing sensitive information such as bank account numbers and Social Security Numbers. Oftentimes the email appears as if it comes from a trusted source. It directs you to a "spoof" website that encourages you to divulge sensitive information. First United Bank will never send you an email asking for confidential information such as account numbers, passwords, PIN numbers, credit card numbers or Social Security Numbers. To ensure that the email is legitimate, contact us immediately.
6. Skimmers are devices used to read the magnetic strip from your credit card or bank card. They are often hidden in places where you legitimately use your card to make a transaction like an ATM or a restaurant. Your information is typically used within 24 hours of the skim to make online purchases.

7. On the phone you may be duped into providing information to someone disguising themselves as a legitimate business representative like your phone company, a department store or cable company.

Ways to Avoid and Monitor Identity Theft:

1. Reconcile your bank and credit card statements monthly. Make sure that there is nothing suspicious or out of the ordinary on your statements. Review your financial statements carefully and question transactions that look unfamiliar. If you don't receive your statement when you're expecting it, contact your financial institution. (Sign up for First United Bank's Free Online Banking service where you will have real-time access to your account information).
2. Guard your Personal Identification Numbers (PIN)s. Do not keep your PIN with any of your credit or ATM cards.
3. Pay bills online or use a locked mailbox to avoid mailbox theft. You are less likely to have your personal information stolen online than from your mailbox. Have your new personal checks delivered to your local financial institution. (Sign up for First United Bank's Bill Pay service today).
4. Report lost or stolen checks or credit cards immediately
5. When mailing your bills, don't leave payment envelopes containing checks in your mailbox; use a secure mailbox.
6. Pay attention to the information that you write on your checks. For example, when you pay your credit card bill, don't list the entire credit card number on the "for" line. For even greater protection, use an online bill payment service. (Sign up for First United Bank's Bill Pay service today).
7. Do not give out personal information such as checking account, credit card or Social Security Numbers over the phone unless you initiated the call. Don't carry your Social Security Card with you and don't print your Social Security Number on your checks.
8. Use your work telephone number instead of your home telephone number.
9. Check your credit report at least once a year. The three major credit-reporting agencies are required to provide you with one free credit report a year. Visit www.annualcreditreport.com to obtain yours. Once you get your report, look at it carefully. Is all your information correct? Are there any accounts or addresses that aren't familiar? Does the number of inquiries seem reasonable? Any unusual information may indicate identity theft. Contact the agency's fraud hotline right away. You also have the option of adding a consumer fraud alert that will require creditors to contact you whenever a new account is opened in your name.
10. Be wary of "phishing" emails that appear to be from a valid company or financial institution requesting confidential information. Legitimate organizations typically do not send unsolicited emails asking for confidential information. Do not reply to these emails or click on links embedded within them. See a sample of a spoof website and a phishing email.
11. Avoid passwords that are easy to discover like your mother's maiden name or your birth date. Regularly change your passwords. Also, create a username that is unique and difficult for others to guess.
12. Shred all documents containing personal information

If you think you are a victim of identity theft, take action immediately. Contact your local police department, First United Bank, the three major credit reporting agencies and the Federal Trade Commission at (877) IDTHEFT. Their website is www.consumer.gov/idtheft.

Credit Reporting Agencies:

Equifax

Report Fraud:

P.O. Box 740241
Atlanta, GA 30374-0241
1-888-766-0008

Order Credit Report:

P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

TransUnion

Report Fraud:

P.O. Box 6790
Fullerton, CA 92634
1-800-680-7289

Order Credit Report:

P.O. Box 1000
Chester, PA 19022
1-800-888-4213
www.transunion.com

Experian

Report Fraud:

P.O. Box 2002
Allen, Texas 75013
1-888-397-3742

Order Credit Report:

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

To order your free Annual Credit Report, contact Central Source:

www.annualcreditreport.com
1-877-322-8228 or 1-877-fact-act

Useful Websites:

www.identitytheft.org
www.privacyrights.org
[www.idtheftcenter.org](http://wwwidtheftcenter.org)
www.consumer.gov/idtheft
www.ftc.gov
www.fdic.gov