Identity Theft

Did You Know?

For criminals, identity theft is a relatively low-risk, high-reward endeavor.

Identity thieves are hard to recognize because they do not necessarily fit a specific profile. An offender could be a complete stranger, a criminally minded cashier or service provider, a neighbor or even a family member.

For victims, however, it can take months or years and thousands of dollars to clear their good name and credit record. In the meantime, they may be refused loans, lose job opportunities and even be arrested for crimes they did not commit. If you are a victim, your best defense is to recognize it quickly and take immediate action to mitigate its effects.
A number of our Prestonwood residents have themselves been victims. If you are prey to this major crime, above all contact the Constable’s office and make a report.

What is Identity Theft?

Identity theft occurs when an individual uses your name, address, Social Security number (SSN), bank or credit card statements or other personal information, to commit fraud or other crimes.

Identity thieves work in many ways. They may:

- Open fraudulent bank or credit card accounts in your name, then write bad checks or incur charges.
- Change your billing address, incur charges on your existing credit card accounts and order new credit cards. Because you never receive the bills, you are unlikely to recognize the problem for some time.
- Use your good credit to secure loans.
- Establish wireless phone service in your name.
- Purchase vehicles by securing vehicle loans in your name.
- Use your name and background information to obtain employment.
- Use your name during an arrest for crimes ranging from traffic violations to felonies. If they are released from custody and fail to appear for their court date, an arrest warrant may be issued in your name.

How Does It Occur?

Identity thieves may use simple or sophisticated means to steal information, such as the following.

- Stealing your wallet or purse.
- Going through trash bins for unshredded credit card and loan applications, discarded credit cards and papers containing personal information such as SSN’s, dates of birth or phone numbers.

ª Stealing newly issued credit cards, utility bill, insurance statements, benefits documents or other information from unsecured mailboxes.

ª Completing a change of address form to divert your mail to another location.

ª Posing as a loan officer, employer or landlord to obtain your credit report.

ª Placing malware (malicious software) on your computer that can steal your user ID’s, passwords, etc.

ª Hacking into computer databases and stealing your personal information.

ª Conducting phone or e-mail scams requesting that you provide personal information to claim a prize or update an account.

ª Stealing files from your employer, merchants, physician’s office or other businesses that maintain your personal records.

ª Shoulder surfing at automated teller machines (ATM) to capture Personal Identification Numbers (PIN).

ª Pretexting/Social Engineering is a practice of obtaining information under false pretenses. For example, the identity thieves claim to be calling from a marketing research firm requesting personal information. The information is used to contact your bank or financial institution.

ª Skimming steals credit or debit and numbers by using a special storage device when processing your card. This usually occurs in restaurants.

ª Phishing occurs when identity thieves send e-mail or pop-up messages pretending to be financial institutions or other legitimate businesses. The e-mails appear to be authentic, but may contain misspelling and/or grammatical errors. They usually request victims to reveal personal information to avoid an account closure or suspension and recent transfers you supposedly performed.

Minimize your risk by managing personal information with care and caution.

ª Reduce access to personal data

ª Protect your SSN

ª Handle credit cards with care

ª Practice smart online shopping

ª Do business with responsible companies

ª Get off promotional lists

ª Monitor financial statements

ª Review your credit report annually

ª Examine your mail

If It Happens to You

ª Inform your bank, creditors and financial institutions that you are a victim.

Ø Ask them to put “fraud alerts” on accounts that have not been compromised

Ø Establish new passwords on all accounts.

Ø Close existing accounts that have been used fraudulently.

Ø Ask them to send you a copy of their fraud dispute form, complete it and return it for processing.

Ø When opening replacement accounts, use new PINs and passwords.

ª Inform the credit reporting agencies that you are a victim of identity theft.

Ø Notify each one by phone and letter.

Ø You can place a 90-day initial fraud alert on your credit report which can be renewed in 90-day intervals indefinitely.

Ø You can also place an extended fraud alert on your credit report for seven years if you provide a police report or other official record showing that you have been the victim of identity theft.

Ø You can freeze your credit report. By freezing your credit report you prevent lenders from seeing your credit report unless you specifically grant them access.

ª Request a free annual credit report. Visit the site at www.annualcreditreport.com.

Ø You are entitled to a free credit report at any time if you have been denied credit, are a victim of identity theft, receive welfare benefits or are unemployed but expect to apply for employment in the next 60 days.

ª Contact the Federal Trade Commission to report the theft and file a complaint. Your information will be included in a database of identity theft cases that, among other things, aids law enforcement agencies’ investigations.

ª Notify your employer if you suspect that your payroll and retirement records have been compromised.

ª Notify the post office if you suspect that your mail has been stolen, that an identity thief has filed a change of your address with the post office or that a thief has used the mail to commit fraud.

ª Contact the Social Security Administration if your Social Security card is lost or your Social Security number has been misused or stolen.

ª Notify check verification companies if your checks have been stolen. Ask them to notify their retail partners. Cancel your existing account and request a new account.

ª Contact your state’s Department of Motor Vehicles office if your driver’s license has been stolen or to see if another license has been issued in your name.

Check Verification Companies

TeleCheck

(800) 710-9898

Certegy, Inc.

(800) 437-5120

Federal Trade Commission

Identity Theft

(877) 438-4338

600 Pennsylvania Ave. N.W.

Washington, DC 20580

www.ftc.gov/idtheft

Social Security Administration

Office of the Inspector General

Fraud Hotline: (800) 269-0271

P.O. Box 17768

Baltimore, MD 21235

www.ssa.gov/oig

U.S. Postal Inspection Service

Mail Fraud

(800) 372-8347

222 S. Riverside Plaza, Ste. 1250

Chicago, IL 60606-6100

www.usps.com/postalinspectors/fraud

Credit Reporting Agencies

Equifax Fraud Division

(800) 525-6285

P.O. Box 740241

Atlanta, GA 30374-0241

www.equifax.com

Experian Fraud Division

(888) 397-3742

P.O. Box 9532

Allen, TX 75013

www.experian.com

TransUnion Fraud Division

(800) 680-7289

P.O. Box 6790

Fullerton, CA 92834-6790

www.transunion.com

Annual Credit Report Request Services

(877) 322-8228

P.O. Box 105283

Atlanta, GA 30348

www.annualcreditreport.com

For more information on ways to protect yourself and your computer from identity thieves and what actions to take if you have become an identity theft victim, visit the Federal Deposit Insurance Corporation (FDIC) web site at www.fdic.gov/consumers/consumer/guard/index.html and click on the multimedia presentation, “Don’t be an on-line victim: How to guard against internet thieves and electronic scams.”

www.usaaedfoundation.org

Dottie Reading, Security

Prestonwood Forest Homeowners Association