TEXAS YOUNG LAWYERS ASSOCIATION
AND STATE BAR OF TEXAS

IDENTITY THEFT GUIDE

IDENTITY THEFT GUIDE

Prepared and distributed as a Public Service
by the
Texas Young Lawyers Association
and the State Bar of Texas
2013

For more information:www.texaslawhelp.org

TABLE OF CONTENTS

IDENTITY THEFT

What Is Identity Theft?

Identity theft is a growing problem in today's information age. Identity theft is a crime that occurs when your personal or financial information is accessed and used without your permission. It is a costly crime, not only because of potential financial loss, but also in terms of the lost time and energy a victim will expend in trying to correct the problems created. Unfortunately, Texas is one of the top states for identity theft. In 2012, there were more than 28,000 reported cases in Texas of identity theft. As of June 2013, Texas ranks fourth in the nation for the highest rate of reported cases of identity theft with 130.3 victims per 100,000 people.

Criminals are becoming more sophisticated in their ability to use your personal information for their gain. A lost or stolen wallet has gone from something that could cost you a few dollars to something that could cost hundreds or even thousands of dollars, not to mention tainted credit.

Thieves today can take your name, birth date, driver's license number, social security number, bank account and other personal information and use it to obtain credit cards or loans in your name. They can even make unauthorized purchases using your current bank accounts and credit cards. The result is that you are out the money that the thief spent and your credit report will become tainted with overdue accounts without your knowledge.

How Does Identity Theft Occur?

Identity thieves often get your information from the trash you throw away. It can come from bank statements, credit card applications, corporate databases, stolen checks, or even from hackers on the internet gaining access to your files on your home computer.

What Are the Different Types of Identity Theft?

There are many different types of identity theft. Most of them can be broken down into financial identity theft, criminal identity theft, or other types of identity theft.

a. Financial identity theft

Many people have financial accounts and some kind of established credit. Criminals will try to manipulate these relationships or create new fraudulent financial relationships with your information. This area of identity theft has the potential to really hurt your financial health and well-being into the future. Criminals will use your social

security number to open new utility, cell phone, or credit card accounts. They also might use your existing accounts and take funds from your accounts or try to obtain loans.

Mortgage fraud is a fast growing type of financial identity theft. A criminal will gain access to your personal information and obtain a mortgage in your name, take the money and then default. The true homeowner could then face foreclosure and eviction. The criminal might offer to help homeowner's make monthly mortgage payments. They then use the victim's social security numbers to commit other types of identity theft and fraud. Identity thieves might also use your personal information to file a bankruptcy case if they need to obtain a discharge of debts incurred in your name or if they want to retaliate against you.

b. Criminal identity theft

Criminal identity theft occurs when someone is stopped by a police officer and gives your identifying information instead of their own. Suddenly, your name, date of birth, driver's license number could all be linked to the particular offense at issue. If they are not arrested at the time, you could find your mailbox filled with notices to appear in court for violations you are not responsible for. You might not even become aware of your new criminal record until you apply for a job, a line of credit, or until a warrant for your arrest is issued. It can be very difficult to clear up this kind of identity theft.

c. Other types of identity theft

Other types of identity theft include Social Security Fraud and IRS/ Income Tax Fraud. If someone takes over your social security number, they could start obtaining your disability, workman's compensation, or health benefits. If someone files their tax return with your identifying information, they could conceal their income and obtain your refund.

Children are also a big target for identity theft as most children do not apply for or check their credit for many years. Sometimes people will file for bankruptcy and use the names and social security numbers of children. Often, the victim will be hesitant to file charges because the criminal is a family member or close friend.

How Do I Know if I Am a Victim?

Identity theft is a unique crime because the victim may not know it has occurred until long after the fact. To catch identity theft early, be on the look out for the following things:

– Unauthorized purchases on bank accounts or credit cards.

– Bills from unauthorized credit accounts.

– Missing bank statements and credit card statements.

– You are turned down for a credit card or loan that you think you should be eligible to receive.

– Unauthorized accounts on your credit report.

How Do I Protect Myself From Identity Theft?

While there is no guaranteed way to prevent thieves from stealing your identity, there are several things you can do to make it harder for them.

– Keep any personal or financial information in a safe and secure place. If you do not need it, shred it.

– Shred any credit card statements, credit card applications, bank statements, bills, or any other pieces of mail that may have identifying information or account information contained in them.

– Memorize your driver's license number, social security number, PIN numbers, and passwords instead of carrying them.

– Shield your hand when entering PIN numbers or signing receipts.

– When creating passwords or PIN numbers, do not use easily obtainable or recognizable numbers such as family names or birthdays.

– Take all credit card receipts and ATM slips and shred them.

– Do not put any unnecessary information on your checks, such as your date of birth or driver's license number.

– Do not have new checks delivered through the mail. Instead, pick them up at your bank.

– Only make purchases at secure websites on the internet.

– Do not enter your personal information on pop up ads or other unsecure websites.

– Do not give out information over the telephone to unknown or unauthorized callers.

– Request a credit report from each of the credit bureaus at least once a year to check for any fraud.

The Texas Office of the Attorney General has developed a kit which may help you if you are a victim of identity theft. You may find the pamphlet at http://www.oag.state.tx.us/ag_publications/pdfs/IDTheft_Affidavit.pdf Doing all these things will help keep you and your identity safe.

What Laws Are In Place to Punish Identity Thieves?

The federal and state legislatures have enacted several laws to punish those who commit identity theft and also help deter future violations. Texas has two major statutes which deal with identity theft.

Texas Penal Code, Section 32.51 makes identity theft punishable as a felony and also gives the court the option to order restitution to the victim. Furthermore, Texas has enacted the Identity Theft Enforcement and Protection Act which among others imposes a duty on businesses to protect and safeguard sensitive personal information. The Texas Attorney General can pursue legal action against those businesses who fail to comply with the Act.

What Are My Remedies if I Am a Victim?
If you believe you have been the victim of identity theft, it is important that you act as quickly as possible. Taking the following steps will help you regain control of your personal information and begin repairing the damage caused by identity thieves.

a. Alert Credit Bureaus

The three major credit bureaus in the United States are Equifax, Experian, and TransUnion. These companies are responsible for maintaining your credit history and information. If someone has stolen your identity, your credit report with one or more of these credit bureaus will often reflect any fraudulent transactions. The fraud units at these credit reporting companies can each be notified in the following ways:

Equifax: By telephone (800) 525-6285 or by mail: P.O. Box 740250, Atlanta, GA 30374-0250. You can obtain a copy of your credit report with Equifax by submitting a written request to P.O. Box 740241, Atlanta, GA 30374-0241, or by calling (800) 685-1111.

Experian: By telephone (888) 397-3742, fax (800) 301-7196, or by mail: P.O. Box 1017, Allen, TX 75013. You can obtain a copy of your credit report with Experian by submitting a written request to P.O. Box 2104, Allen TX 75013, or by calling (888) 397-3742.

TransUnion: By telephone (800) 680-7289 or by mail P.O. Box 6790, Fullerton, CA 92634. You can obtain a copy of your credit report with TransUnion by submitting a written request to P.O. Box 390, Springfield, PA 19064 or by calling (800) 888-4213.

b. Place A Fraud Alert On Your Credit Accounts

A Fraud Alert is a safety mechanism that can protect your credit file when your personal information has been compromised. The Fraud

Alert notifies lenders and other businesses that your credit has been compromised and advises them to take special precautions to ensure your identity before extending credit. A Fraud Alert can provide lenders with additional contact information for you in order to verify that the person applying for credit is actually you. If a Fraud Alert is placed on your credit report with any one of the three major credit reporting companies, then that company will subsequently notify the other two credit bureaus and fraud alerts will be placed on all three credit reports. An Initial Fraud Alert will remain on your credit report for 90 days however it may be renewed if necessary. An Extended Fraud Alert will remain on your file for seven years. If you wish to remove a Fraud Alert from your credit file, you must submit a written request to the credit reporting agency where it was filed.

A Security Freeze (or Credit Freeze) is another way to protect your credit but it carries greater restrictions on your credit file when compared to a Fraud Alert. A Security Freeze will prevent a lender from accessing your credit report altogether, thereby preventing them from extending any credit whatsoever. Once a Security Freeze is placed on your credit report, you will have to take special steps in order to apply for any type of credit. Unlike a Fraud Alert, a Security Freeze must be separately placed on each credit report with the three major credit bureaus if you intend to freeze your entire credit. A Security Freeze also remains on your credit file until you remove it or choose to temporarily lift it when applying for credit or accessing your credit file.

c. Review Your Credit Reports

You should request a copy of your credit reports from the three major credit bureaus and check them for any unusual or abnormal entries. Your credit report will provide you with instructions on how to dispute any fraudulent information contained within your credit report. You should continue to regularly monitor your reports as some fraudulently activity may not occur for months (or even years) after your personal information was compromised.

d. File A Report With Law Enforcement

If you have been the victim of identity theft, you should always make every effort to report the crime to the appropriate investigative agency.

General Identity Theft Crimes – The Federal Trade Commission is the agency generally responsible for receiving and processing complaints from individuals who believe they may be victims of identity theft. The FTC is able to provide helpful materials to identity theft victims and will also refer the complaints to appropriate law enforcement and credit entities. The FTC can be reached online at www.ftc.gov/bcp/edu/microsites/idtheft/, by telephone (toll-free) at (877) 438-4338, or by mail: FTC Identity Theft Clearinghouse,

600 Pennsylvania Avenue, N.W., Washington, DC 20580. The Dallas office of the FTC covers all of Texas: Federal Trade Commission, 100 N. Central Expressway, Suite 500, Dallas, TX 75201, (877) 438-4338, www.consumer.gov/idtheft/.

You can also report general crimes relating to identity theft and fraud to your local FBI (www.fbi.gov/contact/fo/fo.htm), U.S. Secret Service field office (www.secretservice.gov/criminal.shtml/field_offices.shtml), or your local police or sheriff's department.

Identity Theft Involving U.S. Mail – If you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity, you should report the crime to the U.S. Postal Inspection Service (postalinspectors.uspis.gov/forms/IDTheft.aspx).

Identity Theft Involving a Social Security Number – If you suspect that your Social Security number is being fraudulently used, you may report the fraud to the Social Security Administration by calling (800) 269-0271, or by fax (410) 597-0118, or online at www.ssa.gov. If your card has been physically stolen, you will need to apply for a replacement card by completing Social Security Application Form SS-5.

Identity Theft Involving Taxes and Tax Returns – If you suspect that a tax return was fraudulently filed on your behalf or that your identity was otherwise used fraudulently in connection with a tax violation, you should contact the Internal Revenue Service by calling (800) 829-0433 or by going online at http://www.irs.gov/uac/Identity-Protection. You may be required to submit IRS Form 14039, which is an affidavit of identity theft.

Identity Theft Involving Student Loans – If you suspect that an identity thief has obtained a student loan in your name, you should report it, in writing, to the school that opened the loan and request that the account be immediately closed. You should also report the fraud to the U.S. Dept. of Education at (800) 647-8733 or by mail: Office of Inspector General, U.S. Dept. of Education, 400 Maryland Ave., SW, Washington, DC 20202-1510, or online: www.ed.gov/about/offices/list/oig/hotline.html?src=rt.

e. Contact Creditors And Financial Institutions And Close Any Affected Accounts

i. Fraud Alert on Existing Accounts

If you have an existing credit or debit account that was used fraudulently, you should report the fraud immediately to your credit card company and request that they issue you replacement cards with a new account number. You should also follow up with your credit card company, in writing, which should be mailed to the address listed by

your credit card company for "billing inquiries." You will also likely be required to provide your credit card company with a fraud affidavit or a dispute form. You should also consider resetting any passwords or pin numbers associated with the affected accounts.

ii. Stolen Checks And Fraudulent Bank Accounts

If any personal checks have been stolen from you or if you discover that a bank account has been opened fraudulently, you should notify your bank and ask that they issue a "stop payment" on any fraudulent checks. You should also ask your bank to report the fraud to ChexSystems, which is a consumer reporting agency for checking accounts. You can also request that ChexSystems place a security alert on your file: www.consumerdebit.com/consumerinfo/us/en/chexsystems/theftaffidavit/index.htm, or by writing ChexSystems Inc., Attn: Consumer Relations, 7805 Hudson Rd., Suite 100, Woodbury, MN 55125.

iii. Unauthorized Credit Accounts

If your credit report reflects that one or more new credit accounts have been opened in your name by identity thieves, you should contact those creditors immediately by telephone and in writing. Federal law allows you to prevent a business from reporting the fraudulent account(s) to the credit bureaus; however, you may be required to submit a fraud affidavit to the creditor first. You should request, in writing, to the business which extended the fraudulent credit copies of any documentation that was submitted to them by identity thieves, such as the fraudulent application and transaction records. Federal law requires the merchant to provide you with a copy of these records once they are presented with (a) a copy of a FTC affidavit or another acceptable identity theft affidavit, (b) a government-issued identification, and (c) a copy of a police report or identity theft report. The business must provide you with copies of these records within 30 days of the request at no charge. You are also authorized to allow a law enforcement investigator to access to these records from the merchant.

After providing the necessary documentation, you should ask the creditor for a letter stating that the company has closed the disputed account and has discharged the debts.

iv. ATM And Debit Cards

If your ATM or debit card is stolen or otherwise compromised, you should report it to your bank as early as possible. You should also submit a fraud affidavit to your bank and request a new card, account number, and password. If there are any fraudulent transactions, you should review your debit card contract regarding liability. Some cards provide better loss protection against fraudulent transactions than others. Despite being a victim of identity theft, your liability for fraudulent charges may increase the longer the crime goes unnoticed or unreported.

v. Brokerage Accounts

Brokerage accounts do not carry the same level of protection against loss as bank accounts or credit and debit cards accounts. Funds in a brokerage account are only required to be restored in instances when a brokerage firm fails. You should carefully review your agreement with your brokerage firm regarding identity theft and fraud.

f. Dealing With Debt Collectors

If a debt collector contacts you and attempts to collect on an unpaid bill for a fraudulent account, you should:

1. Request (a) the name of the collection company, (b) the name of the person contacting you, (c) the phone number, and (d) their address.

2. Inform the debt collector that you have been a victim of fraud and are not responsible for the account.

3. Request (a) the name and contact information for the referring credit issuer, (b) the amount of the debt, (c) account number, and (d) the specific dates of the charges.

4. Ask the collector if he or she needs you to submit a fraud affidavit or a copy of an FTC affidavit (http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf).

5. Follow up by writing a letter to the debt collector explaining your situation and remember to retain a copy for your records.

6. Ask the collection company to confirm, in writing, that you do not owe the debt and that the account has been closed.

Under federal law, a debt collector is obligated to notify the creditor whenever a debt may be the result of identity theft. The law also prohibits a creditor from attempting to sell or transfer any debt caused by identity theft. For further information on dealing with debt collectors, go to www.privacyrights.org/fs/fs27-debtcoll.htm#8.

For Additional Copies Please Contact:
Public Information Department
State Bar of Texas
P.O. Box 12487
Austin, Texas 78711-2487
(800) 204-2222, Ext. 1800
www.texasbar.com

SB0179E-0314

40316