IDENTITY THEFT AND FRAUD GUIDE

Produced and distributed as a public service by
the Texas Young Lawyers Association and the State Bar of Texas

Note: This Identity Theft and Fraud Guide is not intended to be a fully comprehensive guide to all forms and types of identity theft and fraud, nor is it intended to be legal advice or construed as a legal authority. In the event you feel you are the victim of identity theft, please consult an attorney.

For more information: www.texaslawhelp.org

©2024
Texas Young Lawyers Association

TABLE OF CONTENTS

What Is identity theft?

Identity theft and *identity fraud* are terms used to refer to types of crime in which someone wrongfully obtains and uses another person's personal information or data in some way that involves fraud or deception, typically for economic gain.[1] There are many different types of identity theft and fraud, with the most common being "financial identity theft" and "criminal identity theft." Other forms, however, are becoming increasingly common. These include theft relating to tax returns, estates, real estate, and children, among others; using schemes such as e-mail spoofing, social engineering, pretext calling, romance or grandparent scams, or simply stealing a wallet or rummaging through trash.

No matter the type or cause of the theft or fraud, Texas is one of the top states for identity theft in our country. In 2021, there were more than 101,002 reported cases of identity theft at a rate of 350 reports per 100,000 Texans.[2] 40% involved stolen credit cards, 21% related to loans, and 12% were related to bank accounts.[3] Nearly two out of every 100 residents of our state's four largest metropolitan areas are victims of identity theft in a given year.[4] In 2023, there were more than 47,000 reported cases in Texas of cybercrimes relating to identity theft totaling loses of over $1 billion.[5]

---

[1] "Identity Theft" United States Department of Justice, www.justice.gov. April 2024.

[2] Consumer Sentinel Network: Data Book 2023. Federal Trade Commission. February 2024.

[3] *Id.*

[4] *Id.*

[5] Internet Crime Report. Federal Bureau of Investigation. 2023.

How does identity theft occur?

Identity theft can happen in many ways, such as a stolen or lost wallet that may include your driver's license, credit cards, and other personal identifying information. There are also several common sources of theft that you may not think of. For example, your trash will often contain valuable information such as bank account and credit card numbers, applications for various types of credit, or other documents that may allow a criminal to benefit using your identity. Personal information can also be taken from common items such as checks, court documents, medical forms, school applications, tax returns, surveys or other documents we willingly provide strangers in our daily interactions, often without thinking twice.

In addition to the "old" ways of stealing someone's identity, there are also modern methods that have evolved with technology and social norms. Your social media page, for example, may not only contain a photo of *the best meal you have ever eaten*, but it may also contain references to your birthdate, the names of your elementary and high schools, your home town, your favorite teacher or pet, the street you grew up on, your mother's maiden name (that photo you tagged of grandma) and your favorite sports teams, all answers to questions commonly used to verify identity. There is also, of course, the modern equivalent of a stolen wallet: the stolen or compromised password.

What are the different types of identity theft and fraud?

a. Financial Identity Theft

In today's modern system of commerce, bank accounts, debit cards and credit cards are essential. Therefore, it is no surprise that over 50% of the cases of reported identity theft involve some type of financial product (e.g., credit cards, loans and bank accounts). Criminals tend to strike

where the money or credit is. In the past that would have meant trying to steal physical money from banks. However, while you may still see an occasional story about a bank robbery on the evening news, today's criminals are using your personal information to steal without ever having to leave the comfort of their own homes. They will use "in-wallet information" (i.e., information commonly found on your driver's license or a credit card) and "out-of-wallet information" (i.e., information like your mother's maiden name, high school mascot, or make of your first car) to access existing accounts and create new ones. This area of identity theft has the potential to significantly hurt your financial health and well-being not only today, but well into the future.

In addition to the more common credit card and bank account-related fraud, various types of mortgage and real estate fraud are quickly growing types of financial identity theft. For example, once a criminal gains access to your personal information, they will use that unique information to take out a mortgage loan on your existing home and will subsequently withdraw the funds in full leaving you to face the potential foreclosure and eviction.

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. Without warning, your name, date of birth or driver's license number could all be linked to the offense at issue. If the person pretending to be you is 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. Note: the

possession of a fake ID is a Class C misdemeanor punishable by up to a $500 fine as well as community service. Possession of a stolen ID is potentially a Class A misdemeanor punishable by up to a $4,000 fine and 30 days in jail.

c. Other Types of Identity Theft

Fraud relating to Social Security payments, income taxes, and other government programs that involve payments and subsidies is quite common. These types of fraud are often initiated when your Social Security number is compromised. If the wrong person were to obtain your SSN, they could steal disability, workers' compensation, or health benefits. Similarly, someone could use your SSN to file a fraudulent tax return to either conceal their own income, or even steal your refund.

Children are also an increasingly popular 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, or even use a child's SSN to apply for jobs, apply for government benefits, or open bank accounts and obtain loans. This type of fraud is most commonly perpetrated by family members or close friends of the victim. Children's Social Security numbers are also commonly used in schemes claiming to help individuals "repair their bad credit" by obtaining a replacement Social Security number. In this instance there are two victims: the individual whose Social Security number is stolen, and the individual who unknowingly purchased a stolen SSN. Remember, there is no such thing as a replacement Social Security number.

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 lookout 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.
- Calls and letters from reputable collectors (but watch out for scam calls and letters, too!).
- You are denied a bank account for attempting to open too many credit accounts within the past six months.

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.
- Never carry your Social Security card or Social Security number in your wallet.
- Shield your hand when entering PIN numbers or signing receipts, and do not write your PIN number on your debit and credit cards.
- Instead of signing the back of your debit and credit card, write "Check ID" in the signature block.
- Use unique passwords for every account, and do not use easily obtainable or recognizable numbers such as family names or birthdays.
    - The top five most common passwords in the United States in 2023 were: 123456, password, admin, 1234 and UNKNOWN.[6]
- 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 directly from your bank or credit union.
- Only make purchases at secure websites on the internet from reputable vendors.
- 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. If anyone calls you and asks for your personal information, especially your Social Security number or a password,

[6] Top 200 Most Common Passwords for 2023. nordpass.com/most-common-passwords-list/. April 2023.

even if they claim to be from someone seemingly trustworthy such as a government agency or your financial institution, hang up.

- Enroll in a credit monitoring program.
- Consider placing a "Security Freeze" on your credit report with each of the credit reporting bureaus. See below for more information.
- Request your **FREE** credit report from each of the credit bureaus at least once a year to check for any fraud. You can request your credit report by visiting www.annualcreditreport.com/.

If you are a victim of identity theft, the Texas Office of the Attorney General has developed a kit which may help. You may find the kit at: www.texasattorneygeneral.gov/consumer-protection/identity-theft.

What laws are in place to punish identity thieves?

The federal government and the state of Texas have enacted laws with the intent to curb identity theft and other financial crimes.

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 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. Texas Penal Code Section 32.23 makes it a felony, from a state jail felony (over $2500) to a first-degree felony (over $300,000), for a person to intentionally or knowingly make a materially false or misleading written statement to obtain property or credit from a financial institution, including a mortgage loan.

18 U.SC. § 1028A states "anyone who knowingly transfers, possesses, or uses, a means of identification of somebody shall, in addition to the felony

penalties, will be sentenced to imprisonment of two years, or five years for terrorism." The Bank Secrecy Act is a conglomerate of federal statutes designed to curtail criminal activity through the identification of fraud, protecting consumers from the abuses of financial crime and identity theft. Similarly, the Identity Theft and Assumption Deterrence Act makes it a crime punishable by fine or imprisonment to knowingly and without authorization to use another person's means of identification with the intent to commit a crime.

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, by calling (800) 685-1111, or visiting their website www.equifax.com.

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, by calling (888) 397-3742, or by visiting their website www.experian.com.

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, by calling (800) 888-4213, or by visiting their website www.transunion.com.

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 or credit lock) 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 fraudulent activity may not occur for months (or even years) after your personal information was compromised. As a reminder, you can request your credit report by visiting https://www.annualcreditreport.com.

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 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, consumer.ftc.gov/features/identity-theft.

You can also report general crimes relating to identity theft and fraud to your local FBI (www.fbi.gov/contact-us), U.S. Secret Service field office (www.secretservice.gov/contact/field-offices) 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 Postal Service 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 (www.uspis.gov/tips-prevention/identity-theft).

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 www.irs.gov/identity-theft-central. 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 at: oig.ed.gov/oig-hotline.

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 financial institution or credit card issuer, and request that they issue you replacement cards with a new account number. You should also follow up with your credit card issuer, in writing, which should be mailed to the address listed by your credit card issuer for "billing inquiries." You will also likely be required to provide your credit card issuer 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 used by financial institutions to verify individuals when opening new accounts.

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 write to the business which extended the fraudulent credit and provide copies of any documentation that was submitted 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 an 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 or credit union as early as possible. You should also submit a fraud affidavit to your bank or credit union 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. You may be responsible for any fraudulent charges reported more than 60 days after the fraudulent charge appears on your monthly statement.

v. Brokerage Accounts

Brokerage accounts do not carry the same level of protection against loss as bank accounts or credit and debit card 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 https://www.identitytheft.gov.
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 guides.sll.texas.gov/debt-collection/know-your-rights.

Prepared as a public service by the
Texas Young Lawyers Association
and distributed by the State Bar of Texas

This pamphlet and other free legal resources
can be found online at
texasbar.com/resources.

For additional printed copies please contact
the State Bar of Texas Public Information Department
via email at pamphlets@texasbar.com
or by calling
(800) 204-2222.

Texas Young Lawyers Association
TYLA
BE AN UNCOMMON LEADER®

SB0179E-0314

45492 5/24