

IDENTITY
THEFT



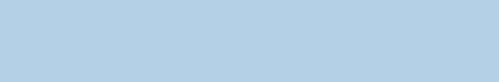
ATTORNEY GENERAL OF TEXAS

GREG ABBOTT

IDENTITY theft

Identity theft can happen to anyone. Previously, criminals stole your wallet for your cash. Now they want your wallet to steal your good name. Protect yourself and your identity.

HOW how TO to AVOID avoid IDENTITY identity THEFT theft



Identity theft occurs when someone uses your personal identifying information without your permission. This information can include your name, address, driver's license number, Social Security number, mother's maiden name, birth date, or financial information such as your bank account, credit card, or PIN number.

An identity thief can obtain your identifying information by stealing credit card applications, bank statements, or checks from your trash or mail, finding your lost or stolen wallet or purse, hacking your credit card number from a corporate database, or stealing your information from inside a company that holds it.

An identity thief can use your information to obtain new credit cards, open checking accounts, get a bogus

driver's license or Social Security card, make long distance calls, apply for a job, or make purchases using your bank account or credit card. Identity theft is a felony crime and should be reported to your local law enforcement agency.

Because of the nature of the crime, you may not realize your identity has been stolen until you are denied credit, turned down for a job, or sent a bill for purchases you did not make. By that time, your good name and credit history may be in ruins. Rebuilding good credit in the aftermath of identity theft can take months or even years.

WARNING SIGNS of identity theft

Warning signs include:

- You receive bills from a credit account you did not open.
- You see unauthorized charges on your credit, long distance, or bank accounts.
- You are contacted by a collection agency regarding a debt you did not incur.
- Checks disappear from your checkbook.
- Bank and credit billing statements don't arrive on time.
- Your credit report shows accounts you did not authorize.
- You are turned down for a credit card, loan, mortgage, or other form of credit due to unauthorized debts on your credit report.

WHAT TO DO IF YOU ARE A VICTIM of identity theft

The Attorney General recommends that you take the following steps if you suspect you are a victim of identity theft:

- File a police report with your local law enforcement agency and keep a copy of that report. Many banks and credit agencies require such a report before they will acknowledge that a theft has occurred.
- Contact the three primary credit reporting bureaus to have a security alert or freeze placed on your report.
- Request a copy of your credit report and review it for unauthorized account activity.
- Report unauthorized charges and accounts to the appropriate credit issuers and credit bureaus immediately by phone and in writing. Cancel the accounts.
- If your wallet or purse is stolen, immediately cancel your credit and debit cards and get replacements. Put a “stop payment” on all lost or stolen checks.

The Federal Trade Commission (FTC) has authority to prosecute identity theft at the federal level. Report identity theft to the FTC by calling (877) IDTHEFT (438-4338), or visit their website at www.ftc.gov.

If you are a victim of identity theft, you may get a call from someone posing as a bank representative or law enforcement official requesting your personal information under some pretext. Do not give out your information – you have no way of knowing who is really on the other end of the line.

If another person is arrested and falsely uses your name or other personal information, Texas law allows you to have your information removed from the arrest record. Contact the Crime Records Service at the Texas Department of Public Safety (DPS) by calling (512) 424-5258, or visit their website at www.txdps.state.tx.us.



CREDIT REPORTING bureaus

Report fraud or request a copy of your credit report by contacting the three primary credit reporting bureaus:

EXPERIAN

P. O. Box 9532

Allen, TX 75013-2104

www.experian.com

(866) 200-6020 (to request credit report)

(888) 397-3742 (to report fraud)

EQUIFAX

P. O. Box 740241

Atlanta, GA 30374-0241

www.equifax.com

(800) 685-1111 (request report)

(800) 525-6285 (report fraud)

TRANS UNION

P .O. Box 2000

Chester, PA 19022-2000

www.transunion.com

(800) 888-4213 (request report)

(800) 680-7289 (report fraud)

When you report fraud to one credit bureau, that report will automatically be sent to the other two agencies. Each company will then place a fraud alert on your account and send you a copy of your credit report for review.

PROTECTING your identity

You can reduce the chance that you will be a victim of identity theft by taking the following precautions:

- Minimize the amount of personal financial information you carry. Memorize passwords and PIN numbers instead of carrying them with you.
- Keep personal financial information in a secure place in your home. Shred identifying information before throwing it away.
- Do not give sensitive information to unsolicited callers. Remember that most legitimate businesses will not ask for your Social Security or bank account numbers.
- Shield your hand when entering your PIN at a bank ATM or when making long distance calls with a calling card. Take your credit card receipts and ATM slips. Shred them before throwing them away.
- Pick up new checks or a new or reissued credit card at your bank rather than having them delivered to your home. Do not have your driver's license number or Social Security number printed on your checks.
- If your bank or credit card statement does not arrive on time, call the issuer to make sure it is being sent to the proper address. Also contact the Post Office to see if a change of address has been filed in your name. A thief might steal or divert your statements to hide illegal credit activity.

DATABASE theft and hacking

Keep your personal financial information off corporate marketing and billing databases as much as possible to reduce the chance that your information will be hacked or stolen. To be removed from many mailing lists for up to five years, sign up online at www.the-dma.org, or write to:

Direct Marketing Association
Mail Preference Service
P. O. Box 643
Carmel, NY 10512

Limit the number of pre-approved credit offers you receive by removing your name from the marketing lists of the three credit reporting bureaus. Call 888-5OPT-OUT (888) 567-8688.

If any of your credit card issuers send random-issue convenience checks, request in writing to be removed from that mailing list.

Ask your bank about its privacy and information policies. Find out under what circumstances your bank may provide your account information to a third party. Request that you be notified in advance and ask if it is possible to opt out of this practice.

SOCIAL SECURITY information

Do not carry your Social Security card with you unless you need it for a job application. Release your Social Security number only when absolutely necessary or when required by law. Ask the requestor if another identification number can be used instead.

Never print your Social Security number on your checks. If your workplace displays your Social Security number on a timecard or other place open to public view, ask to have this procedure changed.

If you are over age 25, you should receive a Social Security statement by mail each year. Check your statement thoroughly and report any inaccuracies to the Social Security Administration. You can order a copy of your statement by calling (800) 772-1213 or by accessing the Social Security website at www.ssa.gov.

CREDIT reports

Order a copy of your credit report at least once a year from each of the three credit bureaus listed in this brochure to check for inaccuracies or fraudulent use of accounts. You can order a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228.

Even if you have not been the victim of identity theft, consider asking the credit bureaus to place a security alert on your account as a protective measure. This alert instructs creditors to call you personally to verify applicant information. While this will mean that you can no longer get instant credit, such as on-site approval for store charge cards, it will also stop others from getting credit in your name. Be sure to ask how long the alert will be in effect and how to extend it if necessary.

CREDIT / ATM / DEBIT CARDS

Reduce the number of credit cards you use and only carry the cards that you intend to use.

Use credit cards that have your photo on them. This makes it more difficult for an imposter to use stolen cards at a store.

If you receive an offer for a pre-approved credit card or loan but aren't interested, shred the application form before throwing it away.

BANK ACCOUNTS and billing statements

Check your bank account and credit billing statements carefully each month for unauthorized activity. If you receive a credit card in the mail that you did not request, call the issuer to find out why it was sent to you. If it was requested by someone else in your name, cancel it immediately.

When creating a password for an ATM card, long distance account, credit card, or other form of credit, do not use common numbers such as your birth date or the last four digits of your Social Security number. Avoid using names, such as your mother's maiden name or your birthplace, that are likely to appear in public records accessible to thieves.

COMPUTER and internet security

If you store financial records on your computer, use passwords and install an electronic firewall to keep burglars and Internet hackers from accessing your computer.

Do not give your credit card number or other financial information over the Internet unless you are certain you have a secure server connection. These usually include an "s" after the "http" web address and a icon of a "closed lock" or "key" at the bottom of the screen.

Save the transaction number or confirmation number provided to you by the business and make a note of the date/time of the transaction and what you ordered.

Review the privacy policy of any online companies you deal with and request that they not share your financial information.

TELEMARKETING
no call lists

Texas No Call

P. O. Box 313

Walpole, MA 02032

(866) 896-6225 toll free

www.texasnocall.com

Federal No Call List

(888) 382-1222 toll free

www.donotcall.gov

CONSUMER
complaints

Federal Trade Commission,

Texas office

100 N. Central Expressway, Suite 500

Dallas, TX 75201

(877) 438-4338

www.consumer.gov/idtheft/

For a consumer complaint form, call the Attorney General's Consumer Protection and Public Health Division at (800) 252-8011 or file a consumer complaint online by visiting our website at www.oag.state.tx.us



GREG ABBOTT
Attorney General
of Texas

CONTACT information

For more information or to obtain copies of brochures, call the Attorney General's Consumer Protection Hotline at (800) 621-0508, or contact your nearest Attorney General regional office.

- Austin: (512) 463-2070
- Dallas: (214) 969-5310
- El Paso: (915) 834-5800
- Houston: (713) 223-5886
- Lubbock: (806) 747-5238
- McAllen: (956) 682-4547
- San Antonio: (210) 225-4191

All consumer complaints must be made in writing. Please call or write for a complaint form. Write to:

Office of the Attorney General
Consumer Protection and
Public Health Division/010
P. O. Box 12548
Austin, TX 78711-2548

Complaint forms and additional information can also be found in the Consumer Protection section of our website, at www.oag.state.tx.us