FIGHTING identity theft

www.texasfightsidtheft.gov

Office of the Attorney General
Identity Theft Victim's Kit

This Identity Theft Victim's Kit can help you with the process of recovering from the identity crime committed against you. While the recovery process can be long and at times frustrating, this kit outlines six specific steps to take and provides vital contact information you will need to address the effects of identity theft.

Your stolen identity may be used in several ways. A criminal might assume your identity in order to gain employment, open bank or credit accounts, or even to evade criminal prosecution. Regardless of how your stolen identity is misused, you should take action immediately. The less time criminals have with your identity, the less damage they can do to your reputation and credit.

State law prohibits the Office of the Attorney General (OAG) from acting as an attorney on behalf of an individual citizen. In some instances, you may want to seek the personal advice of a private attorney. The OAG does accept consumer complaints and provides general information about identity theft. Please visit our website or contact the agency if you have questions regarding this kit.

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

www.texasfightsidtheft.gov

Identity Theft Hotline
(866) 720-8100 or (800) 252-8011

REV 09/10

ID Theft Victim's Kit

Task Checklist

This checklist will help you keep track of your progress as you begin to clear your name. Remember: The less time a criminal has with your identity, the less damage he or she can do to your reputation and credit. You should finish all the tasks described below as quickly as possible.

Remember to keep notes of all your phone calls, including the name, date and time of each conversation you have while trying to clear your name. You will find a call log at the end of this kit.

Step 1 Stop ongoing damage to your credit. Close all bank, credit, utility and service accounts that have been fraudulently opened or compromised. Contact the three major credit bureaus and request that a fraud alert or security freeze be placed on your credit report to stop new accounts from being fraudulently opened in your name.

Step 2 Report identity theft crime to your local law enforcement and request a copy of the police report.

Step 3 Report identity theft crime to the Federal Trade Commission (FTC) and complete the FTC's ID Theft Affidavit.

Step 4 Prevent or curtail further identity theft abuses by contacting other relevant law enforcement or government agencies.

Step 5 Monitor your credit report on an ongoing basis to prevent continued identity theft abuses. If debt collectors harass you as a result of identity theft, file a consumer complaint with the Office of the Attorney General.

Step 6 If necessary, complete an Application Requesting Declaration that Applicant is a Victim of Identity Theft, which is included in this ID Theft Victim's Kit, and file it with a Texas state district court.

Step 1

Stop Ongoing Damage to Your Credit

Close all bank, credit, utility and service accounts that have been fraudulently opened or compromised. Request that a fraud alert or security freeze be placed on your credit report to stop new accounts from being fraudulently opened in your name.

- **Immediately close all accounts that you know were used by a thief or that you suspect have been compromised.**
- **Make a list of all your bank, credit, utility and service accounts.**
- **Get a copy of your credit report and check to see that all accounts shown on the report are accounts which you authorized and that their related information is accurate (such as current balances).**
- **Close any unauthorized accounts that appear on your credit report.**
- **Contact credit bureaus to request that a fraud alert or security freeze be placed on your credit report.**

Closing Accounts

The sooner you detect a problem, the less it can harm you. If you know about a specific account that an identity thief has used or has information about, your first step should be to immediately close that account.

In certain cases – such as, if someone finds your lost wallet and begins to use one of the credit cards it contains – assume that all your accounts are at risk and close them immediately.

To stay organized, make a list of all your bank accounts, credit cards, utilities and service providers and their contact information. Using this list as a guide, contact each institution and explain that you are an identity theft victim and ask to close the account. Most institutions will close the compromised account and issue a new account number with no penalty to you.

After contacting all the companies by phone, follow up by mailing them letters stating the date on which you called each one to tell them you might be a victim of identity theft and indicating that you asked, and the company agreed, to close the account and assign it a new number. Your letter should also detail other specific steps that the company agreed to take on your behalf.

Obtaining a Fraud Alert

After you have closed accounts so that the thieves can no longer use them, take immediate action to prevent them from opening NEW accounts in your name.

First, contact any of the credit bureaus listed at the end of this section and ask them to place a fraud alert on your file. Once this fraud alert is placed on your report, all new creditors who receive a copy of your credit report or credit score will know that you do not authorize the opening of a new account, issuance of a new credit card, or an increase in a credit limit unless the creditor first takes reasonable measures to confirm that the request is truly authorized by you. When requesting a fraud alert, indicate a telephone number where you can be contacted to provide verbal authorization before new lines of credit are issued in your name.

To obtain this alert, also called an "initial fraud alert," call the credit bureau by phone and tell them you believe you have been or may become a victim of fraud or identity theft. This initial alert lasts for 90 days. If you find out that you no longer need the fraud alert, you can call the credit bureau again and terminate it. Even though the law does not require that you request this type of alert in writing, it's always a good idea to follow up your telephone call to the credit bureau with a certified letter, return receipt requested, reiterating your request to have a fraud alert placed on your file. To ensure that all three credit reporting agencies place the alert on your file, mail a copy of your letter to each agency.

Step 1

Credit Reporting Agency Contact Information

Equifax
P.O. Box 7402741
Atlanta, GA 30374
www.equifax.com
Report Credit Fraud:
(800) 525-6285
Request Credit Report:
(800) 685-1111

TransUnion
P.O. Box 2000
Chester, PA 19022
www.transunion.com
Report Credit Fraud:
(800) 680-7289
Request Credit Report:
(800) 888-4213

Experian (TRW)
P.O. Box 2002
Allen, TX 75013
www.experian.com
Report Credit Fraud:
(888) 397-3742
Request Credit Report:
(888) 567-8688

Free Credit Report

Placing a fraud alert on your credit report entitles you to receive a free copy of the report from each credit reporting agency. If it is not offered to you, request it.

Once you receive your report, compare the list of accounts that you previously made with the list of accounts shown on your credit report. If any unfamiliar accounts appear on your credit report, notify that creditor immediately, close the account and dispute the charges. Explain that the account may have been opened without your knowledge by an identity thief. Send a letter to the same effect to the credit reporting agency and request that the information regarding the fraudulent account be permanently removed from your record.

Limitations of a Fraud Alert

Be aware that a fraud alert notifies creditors who access your credit file that you may be a victim of identity theft, but it does NOT prohibit them from accessing your report or from issuing new credit in your name. Therefore, consider asking the credit reporting agencies to place a **"security freeze"** on your credit file. When this freeze is added to your report, all third parties, such as credit lenders or other companies (whose use is not exempt under law) will be unable to access your credit report without your permission. Once you place a freeze on your file, you will need to remove or temporarily lift the freeze anytime you want to apply for credit. Each credit reporting agency has its own process and fee for initiating and lifting a security freeze, so you should contact them individually.

A security freeze can be placed free of charge if you have reported the identity crime committed against you to the police and have a copy of the police report. Without such a report, credit bureaus can charge up to $10 each for you to place or lift a freeze. In the next step, you will find out how to report incidences of identity theft to law enforcement and how to obtain a police report.

Check Verification Contact Information

Shared Check Authorization Network (SCAN)
(800) 262-7771

Chexsystems
Attn: Consumer Relations
7805 Hudson Rd., Ste 100
Woodbury, MN 55125
(800) 428-9623

Telecheck
Attn: Forgery Department
P.O. Box 4451
Houston, TX 77210
(800) 710-9898

Further Precautions Regarding Checking Accounts

As a further precautionary measure, determine if any bad checks have been passed in your name by contacting the Shared Check Authorization Network (SCAN). SCAN can quickly determine whether your checks have been fraudulently used in the United States.

If your checks have been misused, contact the check verification companies listed to the left and ask them to alert retailers to your situation. Each check verification company can ask retailers who use their databases to refuse any checks with compromised account numbers.

Notes:

Step 2

Report Identity Theft Crime to Your Local Law Enforcement Agency

1. Report the crime to your local law enforcement agency.
2. Ask for a copy of the police report and case number.

Most creditors require you to provide a police report when you contest fraudulent charges. Therefore, you must report the crime to your local police or sheriff's department and obtain a copy of the corresponding police report. Even if you do not know who used your information or if your information was used in another state, you can file a complaint with local law enforcement.

Under Chapter 32.51 of the Penal Code, the venue for reporting identity crime is the city or county of residence of the person whose identity was stolen or any county in which an offense was committed. The Texas Identity Theft Enforcement and Protection Act requires peace officers to create a written report and provide a copy of it whenever a person living in their jurisdiction alleges being a victim of identity crime.

Be prepared. Some police departments have special complaint forms to report identity theft. These forms can be obtained online or through the departments' offices. Others will take complaints by phone. Be prepared to tell and show the investigator why you believe you are a victim of identity theft. The more evidence you can give your assigned investigator, the more readily he or she can create a police report for you. Make sure that you ask for a copy of the report. Texas law provides that you are entitled to a copy of it, provided you request it.

Remember to keep the original police report in your files and make extra copies so that you can send them to creditors who request it. Also, remember that an identity theft victim who has a police report can request and lift a security freeze for free, so having this report will save you money.

Step 3

FTC Contact Information

ID Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 25080
www.consumer.gov/idtheft
www.ftc.gov
(877)-ID-THEFT
(877)-438-4338
TDD: (866)-653-4261

Report Identity Theft to the Federal Trade Commission (FTC) and Fill Out the FTC's ID Theft Affidavit.

1. Report your identity theft matter to the FTC.
2. Fill out the FTC ID Theft Affidavit completely and accurately.
3. Submit a copy of the affidavit to creditors who agree to accept it instead of a police report or instead of the creditor's own affidavit form.

Contact the FTC

The FTC maintains a national database of identity theft crimes, which helps lawmakers, consumer protection offices and law enforcement identify trends and investigate identity crime.

To file your identity theft complaint with the FTC, contact the agency directly by telephone, mail or online.

Notes:

Step 3

FTC ID Theft Affidavit

The FTC provides an Identity Theft Affidavit to help victims of identity theft quickly and accurately dispute new unauthorized accounts. It is especially helpful in cases where consumers are unable to file or obtain a police report. Some creditors will accept this affidavit instead of a police report. Also, when you contact creditors to dispute charges based on the fact that you were a victim of identity theft, they will likely require you to complete their own affidavit form, but might accept the FTC's version instead. Using this affidavit form will save you time. Be sure to fill out the affidavit completely and accurately.

The FTC Identity Theft Affidavit can be downloaded from the Office of the Attorney General's website at www.texasfightsidtheft.gov. Remember to use certified mail, return receipt requested, so you can prove your documents were received. Always send copies to creditors and keep originals for your records.

Notes:

FIGHTING

identity theft

www.texasfightsidtheft.gov

Federal Trade Commission

ID Theft Affidavit

Instructions for Completing the ID Theft Affidavit

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened or used in your name that you didn't create the debt. A group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission(FTC) developed an ID Theft Affidavit to make it easier for fraud victims to report information. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it. It will be necessary to provide the information in this affidavit anywhere a new account was opened in your name. The information will enable the companies to investigate the fraud and decide the outcome of your claim. If someone made unauthorized charges to an existing account, call the company for instructions. This affidavit has two parts:

- **Part One** — the ID Theft Affidavit — is where you report general information about yourself and the theft.

- **Part Two** — the Fraudulent Account Statement — is where you describe the fraudulent account(s) opened in your name.

Use a separate Fraudulent Account Statement for each company you need to write to. When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver's license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them. Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation.

ID Theft Victim's Kit

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly. When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe.

Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received.

The companies will review your claim and send you a written response telling you the outcome of their investigation.

Keep a copy of everything you submit.

If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you.

Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report and help stop further fraud.

If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party.

Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

DO NOT SEND AFFIDAVIT TO THE FTC
OR ANY OTHER GOVERNMENT AGENCY

If you haven't done so, report the fraud to the following organizations:

Credit Bureaus

1. Any one of the nationwide credit bureaus to place a fraud alert on your credit report. Fraud alerts can help prevent an identity thief from opening any more accounts in your name. The credit bureau you call is required to contact the other two, which will place an alert on their versions of your report, too.

- **Equifax** (800) 525-6285
  www.equifax.com
- **Experian** (888) EXPERIAN (397-3742)
  www.experian.com
- **TransUnion** (800) 680-7289
  www.transunion.com

In addition to placing the fraud alert, the three consumer reporting companies will send you free copies of your credit reports, and, if you ask, they will display only the last four digits of your Social Security number on your credit reports.

Security or Fraud Department

2. The security or fraud department of each major credit bureaus where you know, or believe, accounts have been tampered with or opened fraudulently. Close the accounts. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures. When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.

Local Law Enforcement

3. Your local police or the police in the community where the identity theft took place to file a report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check **www.naag.org** for a list of state attorneys general.

Federal Trade Commission

4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down and stop identity thieves. The FTC also can refer victims' complaints to other government agencies and companies for further action as well as investigate companies for violations of laws that the FTC enforces.

You can file a complaint online at **www.consumer.gov/idtheft**.
If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: (877) IDTHEFT (438-4338); TTY: (866) 653-4261; or write:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580.

DO NOT SEND AFFIDAVIT TO THE FTC
OR ANY OTHER GOVERNMENT AGENCY

ID Theft Affidavit

Victim Information

(1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as

_____
(First) (Middle) (Last) (Jr., Sr., III)

(3) My date of birth is _____
(day/month/year)

(4) My Social Security number is_____

(5) My driver's license or identification card state and number are_____

(6) My current address is _____

City _____ State _____ Zip Code _____

(7) I have lived at this address since _____
(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was

_____

City _____ State _____ Zip Code _____

(9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

(10) My daytime telephone number is (____)_____

My evening telephone number is (____)_____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

How the Fraud Occurred

Check all that apply for items 11 - 17:

(11) ❑ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

(12) ❑ I did not receive any benefit, money, goods or services as a result of the events described in this report.

(13) ❑ My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were ❑ stolen ❑ lost on or about _____.
(day/month/year)

(14) ❑ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

_____	_____
Name (if known)	Name (if known)
_____	_____
Address (if known)	Address (if known)
_____	_____
Phone number(s) (if known)	Phone number(s) (if known)
_____	_____
Additional information (if known)	Additional information (if known)

(15) ❑ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) ❑ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

_____

_____

_____

_____

_____

(Attach additional pages as necessary.)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Victim's Law Enforcement Actions

(17) (check one) I ❑ am ❑ am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18) (check one) I ❑ am ❑ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (check all that apply) I ❑ have ❑ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ❑ did ❑ did not write a report. *In the event you have contacted the police or other law enforcement agency, please complete the following:*

_____	_____
(Agency #1)	(Officer/Agency personnel taking report)
_____	_____
(Date of report)	(Report number, if any)
_____	_____
(Phone number)	(email address, if any)
_____	_____
(Agency #2)	(Officer/Agency personnel taking report)
_____	_____
(Date of report)	(Report number, if any)
_____	_____
(Phone number)	(email address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) ❑ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

(21) ❑ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

(22) ❑ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith. I also understand that is affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. §1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

_____ _____
(signature) (date signed)

_____
(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____ _____
(signature) (printed name)

_____ _____
(date) (telephone number)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below.**
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

❑ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address *(the company that opened the account or provided the goods or services)*	**Account Number**	**Type of unauthorized credit/goods/services provided by creditor** *(if known)*	**Date issued or opened** *(if known)*	**Amount/Value provided** *(the amount charged or the cost of the goods/services)*
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	auto loan	01/05/2002	$25,500.00

❑ During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address _____

Account number _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Step 4

TXDPS Contact Information

Texas Department of Public Safety Driver License Division

www.txdps.state.tx.us
(512) 424-2600 (English)
(512) 424-7181 (Spanish)

Prevent Further Identity Theft Abuse by Contacting the Following Agencies:

- Local Texas Department of Public Safety Driver License Office
- Social Security Administration (SSA)
- Internal Revenue Service (IRS)
- U.S. Postal Inspection Service
- U.S. Passport Agency

An identity thief might use your personal information to fraudulently obtain a driver's license, file for bankruptcy, apply for Social Security benefits or even get a passport. To head off such possibilities, contact the following agencies and follow their procedures to prevent an identity thief from using your personal information in this manner.

Texas Department of Public Safety Driver License Office

The Department of Public Safety (DPS) can check its database to determine the last time a driver's license was issued in your name. If a license was issued after the last time you obtained one for yourself, immediately report that fraud to DPS. Your local driver's license office will determine the best course of action for your individual situation. To find the location of the nearest driver's license office, contact DPS by telephone or visit the agency's website.

SSA & IRS Contact Information

Office of the Inspector General Social Security Administration

Suite 300 Altmeyer Building
6401 Security Blvd.
Baltimore, MD 21235
www.ssa.gov/oig
(800) 269-0271

Internal Revenue Service

www.irs.gov
(800) 829-1040

Social Security Administration

If you believe your Social Security number has been compromised, immediately contact the Social Security Administration. Order a copy of your Personal Earnings and Benefits Estimate Statement (PEBES) and compare it to your work history. If you notice any employers or earnings you do not recognize, someone might be using your Social Security number for employment. Report any discrepancies to the Social Security Administration's Office of the Inspector General.

In extraordinary circumstances, the Social Security Administration may change your Social Security number. However, changing your number will be done only as a last resort when a very specific set of criteria have been met. Contact the Social Security Administration to determine the best course of action for you.

Internal Revenue Service

If you believe an identity thief has used your Social Security number to fraudulently file for a tax refund or has compromised your taxes, contact your local Internal Revenue Service (IRS) Taxpayer Assistance Center. IRS personnel will help you determine what damage has been done to your tax record and help you determine the steps to correct the problem.

Post Office & Passport Contact Information

United States Postal Inspection Service

Criminal Investigations
Service Center
Attn: Mail Fraud
222 S. Riverside Plaza, Suite 1250
Chicago, IL 60606-6100
www.usps.com
(800) 372-8347

U.S. Department of State National Passport Information Center

http://travel.state.gov/passport
(877) 487-2778

U.S. Postal Inspection Service

If you believe an identity thief stole items from your mailbox, or thieves used the U.S. Postal Service as part of the crime committed against you, report it to the nearest U.S. Postal Inspection Service. The U.S. Postal Inspection Service is the law enforcement branch of the U.S. Postal Service and handles all investigations of U.S. Mail theft and fraud.

U.S. Passport Service

If you believe an identity thief has used your identity to obtain a U.S. Passport in your name, report it to the United States Department of State. The threat of terrorism makes this a critical step. Reporting the crime will cause the passport to be rendered useless to the thief, as it will be invalidated once it has been reported as stolen, missing or fraudulent.

Notes:

Step 5

Credit Report Contact Information

Annual Credit Report Request Service

P.O. Box 105283
Atlanta, GA 30348-5283
www.annualcreditreport.com
(877) 322-8228

Monitor Your Credit Report to Thwart Continued Identity Theft Abuses

Each of the three major consumer credit card bureaus is required to provide you with one free copy of your credit report per year. You can use these free credit reports as a tool to monitor your financial well-being. If you find an account on your credit report that you did not open, contact the creditor. To request your free credit reports, call or write the Annual Credit Report Request Service or visit their website.

Keep track of the dates on which important documents such as bills, financial statements and insurance papers normally arrive at your home. If any of these documents are late, contact the sender and find out why. An identity thief can re-route your mail to another address to hide criminal activity. Remember to keep up with the fraud alert or security freeze you requested from credit bureaus. If necessary, renew the fraud alert when it expires (usually every 90 days) or initiate a security freeze.

You might also be contacted by a debt collector about an account that you disputed because of identity theft. If that happens, dispute the debt in writing with the debt collector. If the collector continues to contact you or harasses you or your family, file a complaint with the Office of the Attorney General by calling (800) 252-8011 or going online at **www.texasattorneygeneral.gov.**

Step 6

OAG & State Bar of Texas

Office of the Attorney General

www.oag.state.tx.us
www.texasfightsidtheft.com
(866) 720-8100
(800) 252-8011

State Bar of Texas

www.texasbar.com
(800) 252-9690

If Necessary, File an Application with Your State District Court Requesting a Court Order Declaring That You are a Victim of Identity Theft

1. **Download, review and complete the Application Requesting Declaration that the Applicant is a Victim of Identity Theft from the OAG ID Theft web site at www.texasfightsidtheft.gov.**
2. **File the application with your district court and request a hearing date.**
3. **Appear in court on the specified date and submit evidence proving you are a victim of identity theft.**

As you work to clear your name, you may find it necessary to obtain a court order declaring that you are a victim of identity theft. This is allowed under the Texas Identity Theft Enforcement and Protection Act, found in Chapter 521 of the Texas Business and Commerce Code. If you are granted this type of court order, you may submit it to governmental entities and private businesses to help correct any records that contain inaccurate or false information which resulted from the identity theft.

The Office of the Attorney General has prepared a do-it-yourself application for a court order, which you can complete and file with your state district court. Necessary forms and instructions can be downloaded from the OAG Identity Theft website **www.texasfightsidtheft.gov** or by calling (800) 252-8011.

You may file these forms in state district court on your own behalf, but you are strongly encouraged to hire an attorney to help you with this process. If you do not have an attorney, the State Bar of Texas can help you find one in your area. Call (800) 252-9690 or visit **www.texasbar.com** for a referral.

FIGHTING

identity theft

www.texasfightsidtheft.gov

Application Requesting Declaration of ID Theft

CAUSE NO. _____

IN THE MATTER OF	§	**IN THE DISTRICT COURT OF**
	§	
_____	§	**_____COUNTY, TEXAS**
	§	
	§	
	§	
	§	**_____ JUDICIAL DISTRICT**

APPLICATION REQUESTING DECLARATION THAT APPLICANT IS A VICTIM OF IDENTITY THEFT

1. I, _____, the applicant, am asking the Court to enter an order under the Identity Theft Enforcement and Protection Act, Section 521.101, Chapter 521 TEX. BUS & COMM. CODE (Vernon 2009) declaring that I am a victim of identity theft. The circumstances I have described below in paragraphs 2 through 5 support this Application.

2. Another person or persons used the following personal identifying information without my authority:

- ❑ my name;
- ❑ my social security number;
- ❑ my date of birth;
- ❑ my mother's maiden name;
- ❑ my government issued identification number;
- ❑ my fingerprints;
- ❑ my voice print;
- ❑ my retina or iris image;
- ❑ my unique electronic identification number, address or routing code;

❑ my financial institution account number or numbers;

❑ my telecommunications identifying information or access device.

The unauthorized use of this personal identifying information caused injury and harm to my name, reputation, rights, interests and/or property associated with my name and personal identifying information.

3. I have filed an identity theft complaint with the following law enforcement agency or agencies on the dates shown:

	Law Enforcement Agency	Date
(a)	_____	_____
(b)	_____	_____

4. On _____, 20____, I received information from the offices of law enforcement agencies where I filed my identity theft complaint(s) and they have informed me of the following:

❑ They have **NOT** been able to identify any of the person or persons who used my personal identifying information. **[OR]**

❑ The person or persons who used my personal identifying information were identified and charged with the felony offense of "Identity Theft" pursuant to Section 32.51 of the Texas Penal Code and those charges

- ❑ are still pending; OR
- ❑ have resulted in a conviction; OR
- ❑ were dismissed.

5. As of ——————, 200__, I have received information regarding the following unauthorized transactions in which my name or other personal identifying information was used

without my authorization:

- ❑ Unauthorized transaction using a check to take money from my bank account(s);
- ❑ Unauthorized transaction using a debit card to take money from my bank account(s);
- ❑ Unauthorized transaction charging my credit card account(s);
- ❑ Unauthorized transaction obtaining a credit card account using my name;
- ❑ Unauthorized transaction opening a bank account using my name;
- ❑ Unauthorized transaction establishing a utility account using my name;
- ❑ Unauthorized transactions to obtain goods using my name;
- ❑ Unauthorized transactions to obtain a service using my name;
- ❑ Unauthorized transactions to obtain insurance using my name;
- ❑ Unauthorized transactions to obtain a loan or an extension of credit using my name;
- ❑ Unauthorized transactions or events obtaining or using a driver's license, passport or other identification documents using my name;
- ❑ Unauthorized transactions or events related to obtaining or using a Social Security Card using my name;
- ❑ Other unauthorized transactions:_____

  _____

  _____

  _____

  _____.

6. My personal identifying information and information regarding specific accounts and transactions is not detailed in this application in order to protect the confidentiality of that information.

7. I have not been informed about any other unauthorized transactions. In the event that I receive information regarding other unauthorized transactions before the date that this Court has a hearing to consider my application, I am asking the Court to allow me to present evidence of those additional unauthorized transactions at the hearing.

8. I have been informed that the Court will give notice to me about the date and time for a hearing on my application. At that hearing, I understand that I will be required to present evidence of each of the unauthorized transactions which I have listed above.

9. I am requesting that this Court set this matter for hearing and that after giving notice of the date and time for that hearing, that the Court enter an order declaring that I am a victim of identity theft because I have been injured by violations of Section 521.051, TEX. BUS & COMM. CODE (Vernon 2009) and/or Section 32.51 TEX. PENAL CODE. For the Court's convenience, I have attached relevant portions of the Texas Identity Theft Enforcement and Protection Act to my application.

Respectfully submitted,

_____
(signature of applicant)

_____
(printed name of applicant)

_____
(street or p. o. box mailing address)

_____
(city, state and zip code)

_____
(telephone number)

FIGHTING

identity theft

www.texasfightsidtheft.gov

Court Order Application

Instructions for Preparing & Filing the Application for a Court Order

Before you begin to fill out the court order application, take time to review and copy it. Also, it will be much easier for you to fill out the application if you first gather relevant documents such as copies of identity theft complaints that you have filed and information reflecting account numbers, transactions and events in which you were a victim of identity theft. For your convenience, each of the following instructions corresponds to a specific section or paragraph of the court order application:

Instruction for filling out the top of the application:

At the top of the application, under the "IN THE MATTER OF" heading, fill in your full name since you are the identity theft victim who is filing this application. Also, fill in the name of the county where you live since that is where you will be filing this application. To file your application, you will go to the office of the district clerk at your county courthouse. There the clerk will give you a "Cause number" and "Judicial district" numbers to fill in the remaining blanks.

Instruction for paragraph 1:

Enter your full name.

Instruction for paragraph 2:

In this paragraph you are telling the court which portions of your personal information (for example, Social Security or driver's license numbers) were used without your approval. Check each and every box that applies to your circumstances.

Instruction for paragraph 3:

In this paragraph you are providing information to the court regarding whether you filed an identity theft complaint with a law enforcement agency and telling the court where and when you filed such a complaint or complaints. Remember that the judge will later have a hearing to consider your application and at that time you will need to present a copy of each such complaint to the judge.

Instruction for paragraph 4:

In this paragraph you are providing information to the court regarding the status of any identity theft criminal complaints you have filed. If you do not know what has happened as a result of your filing a complaint, you may need to contact the law enforcement agency where you filed to find out what has happened as a result of your complaint, including whether or not they have been able to identify the person or persons who used your information. Based on what they tell you, you will check ONLY the boxes that fit your circumstances. Also, fill in the date that law enforcement provided you with the information that you include in this paragraph.

Instruction for paragraph 5:

At the beginning of this paragraph, enter the date that you fill out the application. In this paragraph, you are telling the court about each type of unauthorized transaction in which your name or other information was used without your authorization (for example, an unauthorized transaction establishing a utility account using your name). Only check those boxes which generally reflect transactions or events in which your information was used without your permission. If your information was used in a way that is not already described, there are blank spaces provided at the end of paragraph five where you can explain specifics of what happened in your case.

Instruction for paragraphs 6,7,8,& 9:

Read these paragraphs carefully. They explain that this application does not include specific information (such as your account numbers) in order to protect the confidentiality of that information but that you understand that when the court holds a hearing on your application, you will be prepared to present evidence of each of the unauthorized transactions which you listed in this application. Because the law requires the court to enter specific findings, for each account or transaction that you checked off in paragraph five, you will need to have the following information and related documents to present when you appear before the court: (1) the name of the institution, merchant or business where information was used without your authorization; (2) any relevant account numbers; (3) the dollar amount of the accounts or transactions affected; (4) the date or dates that your information was used without your authorization; and (5) information you may have (if any) identifying the person or persons who used your personal identifying information.

Instruction for the signature block at the end:

You must sign this application and include your printed name, complete mailing address and telephone number. Be sure to provide a correct address and telephone listing because this is how the court's staff will contact you. Failure to accept delivery or pick up mail addressed to you is generally treated by the courts as if you received that mail.

Filing your application:

Once you have completed your application, review it to be sure it is accurate, sign the original and attach to it a copy (provided here) of relevant portions of the Act. Make a copy for your file. Then take your original and copy to the office of the district clerk at your county courthouse. Explain to the staff in that office that you wish to file this application. Your application is being filed pursuant to a law which went into effect on September 1, 2005. If the District Clerk's office is unfamiliar with this type of proceeding, you may need to show them the copy of the law which is attached to your application noting that Section 48.202(a) provides that these types of applications are to be filed in district court. When you file your application, the clerk will keep the original and you should ask the clerk to stamp your copy as "filed." Keep that copy for your records. At the time that you file your application, you must also be prepared to pay a filing fee to the office of the district clerk.

Notes:

CAUSE NO. _____

IN THE MATTER OF	§	**IN THE DISTRICT COURT OF**
	§	
_____	§	**_____COUNTY, TEXAS**
	§	
	§	
	§	
	§	**_____ JUDICIAL DISTRICT**

PROPOSED
ORDER DECLARING A VICTIM OF IDENTITY THEFT

On _____ (date), this Court held a hearing to consider the Application Requesting Declaration That Applicant Is a Victim of Identity Theft filed by_____ (hereafter "Applicant"). Notice of this hearing was provided to the Applicant who appeared and represented himself **[or]** was represented by his attorney of record.

FINDINGS OF THE COURT

After giving due notice of this hearing and considering the application filed in this matter together with all the evidence submitted at such hearing, the Court finds: (1) that all persons entitled to notice of this hearing were properly cited; (2) that it has jurisdiction of this matter; (3) that all legal requirements for issuing this Order Declaring that Applicant is a Victim of Identity Theft have been met; (4) that a preponderance of the evidence demonstrates that applicant has been injured by a violation of Section 521.051, Tex. Bus & Comm. Code (Vernon 2009) or is a victim of identify theft resulting from an offense under Section 32.51 of the Texas Penal Code; and (5) this Court maintains jurisdiction of this matter and at any time may vacate this order if the court finds that the application filed or any information submitted to the court by the applicant contains a fraudulent misrepresentation or a material misrepresentation of fact.

PURPOSE OF ORDER

The Court hereby enters this Order declaring Applicant has been injured by a violation or violations of Section 521.051, Tex. Bus & Comm. Code (Vernon 2009) or is a victim of identity theft from an offense or offenses under Section 32.51 of the Texas Penal Code. As provided by Section 521.101, Tex. Bus & Comm. Code (Vernon 2009) this order may be utilized by Applicant for any of the following purposes: (1) submitting a copy to a governmental entity or private business in order to a correct any record of the entity or business that contains inaccurate or false information as a result of the violation or offense; (2) to prove that a financial transaction or account of the applicant was directly affected by a violation of Chapter 521, Tex. Bus & Comm. Code (Vernon 2009); (3) to prove that a financial transaction or account of the applicant was directly affected by an offense committed under Section 32.51 of the Texas Penal Code; and (4) for use in a civil proceeding brought by or against the applicant arising or resulting from a violation of Chapter 521, Tex. Bus & Comm. Code (Vernon 2009), including a proceeding to set aside a judgment obtained against the applicant.

EXHIBITS

With respect to each financial account or transaction reviewed by the Court and found to be affected by the identity theft, the Court has made specific findings which are recited in Exhibits 1 through ____. The Court hereby orders that each of those exhibits shall be attached to this order and incorporated for all purposes. Each such exhibit references a separate violation or offense and as to each such violation or offense sets forth the following information as required by Section 521.101, Tex. Bus. & Comm. Code (Vernon 2009): (1) any known information identifying the violator or person charged with the offense; (2) the specific personal identifying information and any related document used to commit the alleged offense; and (3) information identifying any financial account

or transaction affected by the alleged violation or offense including the name of the financial institution, any relevant account numbers, the dollar amount of the account or transaction affected by the alleged violation or offense and the date of the alleged violation.

ORDER TO BE SEALED

As required by Section 521.101, Tex. Bus. & Comm Code (Vernon 2009), this Order, including Exhibits 1 through ____ is sealed because of the confidential nature of the information which it includes and may be unsealed only as provided by Section 521.101 and Section 521.101 Tex. Bus. & Comm Code (Vernon 2009). This Order incorporates each of the attached Exhibit(s) 1 through ___ in order to facilitate and enable the victim to furnish a copy of the Order and a copy of an incorporated Exhibit that identifies a separate violation or offense without disclosing confidential information that identifies another violation or offense and another governmental entity or private business in another incorporated Exhibit.

All other relief not hereby granted is denied.

Signed on _____, 20____.

_____
DISTRICT JUDGE PRESIDING

FIGHTING

identity theft

www.texasfightsidtheft.gov

Preparing Exhibits

Instructions for Preparing Exhibits

The Identity Theft Enforcement and Protection Act requires the judge who holds the hearing to consider your application and make very specific findings regarding each financial account or transaction which your application states was affected by identity theft. You can use the Exhibit form to help you prepare for the hearing and to assist the judge in understanding your facts and entering these specific findings. Thus, you should make several copies of the blank exhibit form and fill one out for every instance of identity theft you will present to the court. To assist you in preparation, attach to each exhibit, copies of any documents which you will ask the judge to review. The judge will then be able to review each exhibit together with any documents and testimony you present regarding such exhibit. The judge will then decide as to each exhibit whether you have been a victim of identity theft. If the judge agrees with you that a particular exhibit and the evidence you present demonstrate you are a true victim of identity theft with respect to the particular matter represented in the Exhibit, the judge will attach that exhibit to any final order entered by the court. The judge may decide to attach one, none or all of the exhibits you prepare to the final order. The judge may also elect to modify these exhibits as well as the proposed order that is part of this package to fit your specific circumstances. As required by state law, the Order and all of the Exhibits attached by the judge will be sealed and not open to the public.

CAUSE NO. _____

IN THE MATTER OF	§	**IN THE DISTRICT COURT OF**
	§	
_____	§	**_____COUNTY, TEXAS**
	§	
	§	
	§	
	§	**_____ JUDICIAL DISTRICT**

EXHIBIT ___ of ____

INCORPORATED TO ORDER DECLARING APPLICANT IS VICTIM OF IDENTITY THEFT

On _____, the Court entered an Order Declaring that _____ is a victim of Identity Theft. With respect to each financial account or transaction reviewed by the Court and found to be affected by the identity theft, the Court has attached Exhibits 1 through ____ each of which includes specific findings regarding such account or transaction. Having a separate exhibit with specific findings regarding each affected account or transaction will enable the victim to utilize the Court's order to correct inaccurate or false information by furnishing a copy of the Order and a copy of a specific exhibit that relates to a specific offense to a private business or governmental entity without disclosing other confidential information related to a different transaction or account.

1. In addition to the findings in the Order Declaring a Victim of Identity Theft, the Court, with respect to account number _____ finds the following:

(A) the account was established with the following financial institution or merchant: _____.

(B) the dates of the alleged offense and the dollar amounts of the account or transaction were:

Dates:	**Dollar Amounts:**
_____	_____
_____	_____
_____	_____
_____	_____

2. With respect to this account number and the offenses described above, the Court finds that as of the date of entry of this Order, there is no information identifying the violator or persons responsible for this identity theft. **[OR]**

With respect to this account number and the offenses described above, the Court finds that the following information is known identifying the violator or persons responsible for this identity theft:

_____

_____

_____

_____.

3. With respect to this account number and the offenses described above, the Court finds that the following personal identifying information of the victim was utilized to commit the identity theft:

___ state drivers license # _____;

___ social security number _____;

___ birth certificate reflecting date and place of birth of victim;

___ passport number _____ ;

___ other government issued identification: _____;

___ mother's maiden name _____;

___ victim's finger prints;

___ victim's voice prints;

___ victim's retina or iris image;

___ victims other unique biometric data: _____;

___ unique electronic identification number, address or routing code: _____.

4. With respect to this account number or transaction and the offenses described above, the Court finds that the following generally described documents were utilized to commit the identity theft:

_____

_____

_____

_____.

5. With respect to the identity theft described in this Exhibit ___, the Court also finds the following information which further describes the transaction affected by the offense:

_____

_____

_____

_____.

6. As provided by Section 521.101, TEX. BUS. & COMM. CODE (Vernon 2009), this Court's order and Exhibits may be used for the purpose of submitting it to a governmental entity or private business in order to:

(A) prove that a financial transaction or account of the victim was directly affected by a violation of Chapter 521, TEX. BUS. & COMM CODE (Vernon 2009) or the commission of an offense under Section 32.51, TEX. PENAL CODE; or

(B) correct any record of the entity or business that contains inaccurate or false information as a result of the violation or offense.

It may also be used in a civil proceeding brought by or against the applicant arising or resulting from a violation of Chapter 521, TEX. BUS. & COMM. CODE (Vernon 2009), including a proceeding to set aside a judgment obtained against the victim.

7. This Exhibit is attached and incorporated for all purposes to Order Declaring Applicant is a Victim of Identity Theft which was entered this ___ day of _____, 20____.

_____
DISTRICT JUDGE PRESIDING

Effective: April 1, 2009

Vernon's Texas Statutes and Codes Annotated Currentness
Business and Commerce Code (Refs & Annos)
Title 11. Personal Identity Information
Subtitle B. Identity Theft
Chapter 521. Unauthorized Use of Identifying Information
Subchapter A. General Provisions
§ 521.001. Short Title

This chapter may be cited as the identity theft enforcement and protection act.

Effective: September 1, 2009

§ 521.002. Definitions

(a) In this chapter:

(1) "Personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:

(A) name, social security number, date of birth, or government-issued identification number;

(B) mother's maiden name;

(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

(D) unique electronic identification number, address, or routing code; and

(E) telecommunication access device as defined by Section 32.51, Penal Code.

(2) "Sensitive personal information" means, subject to Subsection (b):

(A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(i) social security number;

(ii) driver's license number or government-issued identification number; or

(iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(B) information that identifies an individual and relates to:

(i) the physical or mental health or condition of the individual;

(ii) the provision of health care to the individual; or

(iii) payment for the provision of health care to the individual.

(3) "Victim" means a person whose identifying information is used by an unauthorized person.

(b) For purposes of this chapter, the term "sensitive personal information" does not include publicly available information

that is lawfully made available to the public from the federal government or a state or local government.

Effective: April 1, 2009

§ 521.051. Unauthorized Use or Possession of Personal Identifying Information

(a) A person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.

(b) It is a defense to an action brought under this section that an act by a person:

(1) is covered by the Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.); and

(2) is in compliance with that Act and regulations adopted under that Act.

(c) This section does not apply to:

(1) a financial institution as defined by 15 U.S.C. Section 6809; or

(2) a covered entity as defined by Section 601.001 or 602.001, Insurance Code.

Effective: September 1, 2009

§ 521.052. Business Duty to Protect Sensitive Personal Information

(a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

(b) A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:

(1) shredding;

(2) erasing; or

(3) otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means.

(c) This section does not apply to a financial institution as defined by 15 U.S.C. Section 6809.

(d) As used in this section, “business” includes a nonprofit athletic or sports association.

Effective: September 1, 2009

§ 521.053. Notification Required Following Breach of Security of Computerized Data

(a) In this section, “breach of system security” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system

security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

(b) A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any resident of this state whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(c) Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(d) A person may delay providing notice as required by Subsection (b) or (c) at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.

(e) A person may give notice as required by Subsection (b) or (c) by providing:

(1) written notice;

(2) electronic notice, if the notice is provided in accordance with 15 U. S.C. Section 7001; or

(3) notice as provided by Subsection (f).

(f) If the person required to give notice under Subsection (b) or (c) demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:

(1) electronic mail, if the person has electronic mail addresses for the affected persons;

(2) conspicuous posting of the notice on the person's website; or

(3) notice published in or broadcast on major statewide media.

(g) Notwithstanding Subsection (e), a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.

(h) If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required by this subsection without unreasonable delay.

Effective: April 1, 2009

§ 521.101. Application for Court Order to Declare Individual a Victim of Identity Theft

(a) A person who is injured by a violation of section 521.051 or who has filed a criminal complaint alleging commission of an offense under Section 32.51, Penal Code, may file an application with a district court for the issuance of an order declaring that the person is a victim of identity theft.

(b) A person may file an application under this section regardless of whether the person is able to identify each person who allegedly transferred or used the person's identifying information in an unlawful manner.

Effective: April 1, 2009

§ 521.102. Presumption of Applicant's Status as Victim

An applicant under section 521.101 is presumed to be a victim of identity theft under this subchapter if the person charged with an offense under Section 32.51, Penal Code, is convicted of the offense.

Effective: April 1, 2009

521.103. Issuance of Order; Contents

(a) After notice and hearing, if the court is satisfied by a preponderance of the evidence that an applicant under Section 521.101 has been injured by a violation of Section 521.051 or is the victim of an offense under Section 32.51, Penal Code, the court shall enter an order declaring that the applicant is a victim of identity theft resulting from a violation of Section 521.051 or an offense under Section 32.51, Penal Code, as appropriate.

(b) An order under this section must contain:

(1) any known information identifying the violator or person charged with the offense;

(2) the specific personal identifying information and any related document used to commit the alleged violation or offense; and

(3) information identifying any financial account or transaction affected by the alleged violation or offense, including:

(A) the name of the financial institution in which the account is established or of the merchant involved in the transaction, as appropriate;

(B) any relevant account numbers;

(C) the dollar amount of the account or transaction affected by the alleged violation or offense; and

(D) the date of the alleged violation or offense.

Effective: April 1, 2009

§ 521.104. Confidentiality of Order

(a) An order issued under section 521.103 must be sealed because of the confidential nature of the information required to be included in the order. The order may be opened and the order or a copy of the order may be released only:

(1) to the proper officials in a civil proceeding brought by or against the victim arising or resulting from a violation of this chapter, including a proceeding to set aside a judgment obtained against the victim;

(2) to the victim for the purpose of submitting the copy of the order to a governmental entity or private business to:

(A) prove that a financial transaction or account of the victim was directly affected by a violation of this chapter or the commission of an offense under Section 32.51, Penal Code; or

(B) correct any record of the entity or business that contains inaccurate or false information as a result of the violation or offense;

(3) on order of the judge; or

(4) as otherwise required or provided by law.

(b) A copy of an order provided to a person under Subsection (a)(1) must remain sealed throughout and after the civil proceeding.

(c) Information contained in a copy of an order provided to a governmental entity or business under Subsection (a)(2) is confidential and may not be released to another person except as otherwise required or provided by law.

Effective: April 1, 2009

§ 521.105. Grounds for Vacating Order

A court at any time may vacate an order issued under section 521.103 if the court finds that the application filed under Section 521.101 or any information submitted to the court by the applicant contains a fraudulent misrepresentation or a material misrepresentation of fact.

Effective: April 1, 2009

§ 521.151. Civil Penalty; Injunction

(a) A person who violates this chapter is liable to this state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring an action to recover the civil penalty imposed under this subsection.

(b) If it appears to the attorney general that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the attorney general may bring an action in the name of the state against the person to restrain the violation by a temporary restraining order or by a permanent or temporary injunction.

(c) An action brought under Subsection (b) must be filed in a district court in Travis County or:

(1) in any county in which the violation occurred; or

(2) in the county in which the victim resides, regardless of whether the alleged violator has resided, worked, or transacted business in the county in which the victim resides.

(d) The attorney general is not required to give a bond in an action under this section.

(e) In an action under this section, the court may grant any other equitable relief that the court considers appropriate to:

(1) prevent any additional harm to a victim of identity theft or a further violation of this chapter; or

(2) satisfy any judgment entered against the defendant, including issuing an order to appoint a receiver, sequester assets, correct a public or private record, or prevent the dissipation of a victim's assets.

(f) The attorney general is entitled to recover reasonable expenses, including reasonable attorney's fees, court costs, and investigatory costs, incurred in obtaining injunctive relief or civil penalties, or both, under this section. Amounts collected by the attorney general under this section shall be deposited in the general revenue fund and may be appropriated only for the investigation and prosecution of other cases under this chapter.

(g) The fees associated with an action under this section are the same as in a civil case, but the fees may be assessed only against the defendant.

Effective: April 1, 2009

§ 521.152. Deceptive Trade Practice

A violation of section 521.051 is a deceptive trade practice actionable under Subchapter E, Chapter 17. [FN1]

Telephone Call Log

Use this log to record names, telephone numbers, dates, times and notes from each call you make while trying to clear your name. Keeping all of this information in one place will make it easier to remember what steps you need to take next and track your progress through the recovery process. Download extra telephone call logs at **www.texasfightsidtheft.gov** or request them by calling (800) 252-8011.

Agency or Business Name: _____

_____

Phone Number: _____

Representative's Name: _____

Date: _____/_____/_____ **Time:** _____

Notes:_____

_____

_____

_____

Agency or Business Name: _____

_____

Phone Number: _____

Representative's Name: _____

Date: _____/_____/_____ **Time:** _____

Notes:_____

_____

_____

_____