ARIZONA
ATTORNEY GENERAL'S
OFFICE

1275 West
Washington St.
Phoenix, AZ 85007
602.542.5025

400 West Congress
South Building
Suite 315
Tucson, AZ 85701
520.628.6504

Outside the
Phoenix
or Tucson
metro area
800.352.8431

www.azag.gov/
identity-theft

IDENTITY THEFT REPAIR KIT

Subject:

IDENTITY THEFT

Brought to you by:

ARIZONA ATTORNEY GENERAL MARK BRNOVICH

ARIZONA IDENTITY THEFT COALITION

WARNING: fastest growing white-collar crime in the US


KNOW HOW TO
PROTECT YOURSELF

Message from Attorney General Mark Brnovich

Identity theft: it's a growing problem and it's not going away. As your Attorney General, I want to help protect you from becoming a victim.

Locking your door when you leave home or when you get in and out of your car is second-nature for most of us. However, securing your personal information such as your social security number, credit and debit card information, insurance cards, and other sensitive materials is just as important.

Always review your bank, insurance, and credit card statements as well as any other bills you may receive. Be on the lookout for unusual or suspicious activity.

Review your credit report on a regular basis. You are entitled to one free credit report from each of the three major credit reporting services in the United States (Experian, TransUnion, and Equifax) during a 12-month period.

Never give sensitive information over the phone and only use reputable, trusted merchants when making purchases online. Look for icons such as a padlock or unbroken key at the top of your browser as a sign that encryption is used and the retail site is secure.

Be guarded with your social security number. Only provide your social security number on official government documents. You may be asked to provide your social security number to businesses that need to verify your identity in order to conduct major financial transactions (such as insurance companies, credit card companies, real estate purchases, or major car purchases.) You can refuse, but businesses may refuse to do business with you. Ask questions and never provide this information over the phone.

If you believe you are the victim of identity theft, you should: contact a major credit bureau, your bank or credit union, credit card providers, and any other business or institution that may be directly affected and immediately notify them of the theft. You can also contact one of the nationwide credit reporting agencies to place a fraud alert on your credit. This is a free service and while this is an effective tool to stop someone from opening new lines of credit in your name, this may not prevent the misuse of your existing accounts.

You should also contact your local law enforcement office and report the identity theft. It is important that you obtain a police report or a report number. This report will then help you when working with companies to repair any potential damages to your credit.

Finally, you should contact the Federal Trade Commission (FTC) and file an Identity Theft Affidavit either online (www.identitytheft.gov) or toll free at 1(877) ID-THEFT. In order to complete your FTC Identity Theft Report you will need a copy of the police report or the report number.

Sincerely,

Mark Brnovich

Attorney General Mark Brnovich

Table of Contents

YOU ARE A VICTIM OF IDENTITY THEFT

Someone has obtained access to your checking account, stolen your debit card or ruined YOUR CREDIT HISTORY

MAIL THEFT

WHAT HAPPENED?

You are a victim of identity theft. Someone has obtained access to your checking account or stolen your debit card. Someone has ruined your credit history by opening credit accounts in your name that haven't been paid off. Someone has obtained your credit card number by stealing it, hijacking your computer or any number of other ways. Someone has used your personal information to conduct illegal activities. Now that your credit history is ruined and you are in debt for things you never knew about, you can't qualify for an auto loan to buy a car or pay for those perfect shoes. You could be in danger of being arrested for something you didn't do.

Now what?

WHAT IS IDENTITY THEFT?

Identity theft is when someone fraudulently uses your personal identifying information to obtain credit, take out a loan, open accounts, get identification or numerous other things that involve pretending to be you.

It is a very serious crime that can cause severe damage to your financial well-being if not taken care of promptly. People can spend months and thousands of dollars repairing the damage done to their credit history and name by an identity thief.

Even scarier, some cases of identity theft are connected to more serious crimes that may lead law enforcement to suspect you of a crime you did not commit.

How Do They Get My Personal Information?

Identity thieves can obtain your personal information in a number of ways:

- **Finding personal information you share on the Internet;**
- **"Dumpster diving"** or going through your trash looking for personal information;
- **Stealing your mail;**
- **Stealing your wallet or purse;**
- **Stealing your debit or credit card numbers through "skimming,"** using a data storage device to capture the information at an ATM or during an actual purchase;
- **"Phishing,"** a scam in which the identity thief sends an email falsely claiming to be from a legitimate organization, government agency or bank to lure the victim into surrendering personal information such as a bank account number, credit card number or passwords. Often the email will send you to a phony or spoof Web site that looks just like the real business or government agency – only an expert can tell the difference;
- **Obtaining your credit report** through posing as your employer or landlord;
- **"Business record theft"** involves the theft of files, hacking into electronic files or bribing an employee for access to files at a business;
- **Diverting your mail to another location** by filling out a "change of address" form.

What Do They Do With It?

- **Drain your bank account with electronic transfers, counterfeit checks or your debit card;**
- **Open a bank account in your name and write bad checks;**
- **Open a credit card account that never gets paid off,** affecting your credit report;
- **Use your name if they get arrested** so it goes on your record;
- **Use your name for purchases involved in illegal activities,** such as products for methamphetamine production or an Internet domain for a child pornography site;
- **Use your name to file for bankruptcy or avoid debts;**
- **Obtain a driver's license with your personal information;**
- **Buy a car and use your information and credit history to get a loan;**
- **Obtain services in your name,** such as phone or Internet.

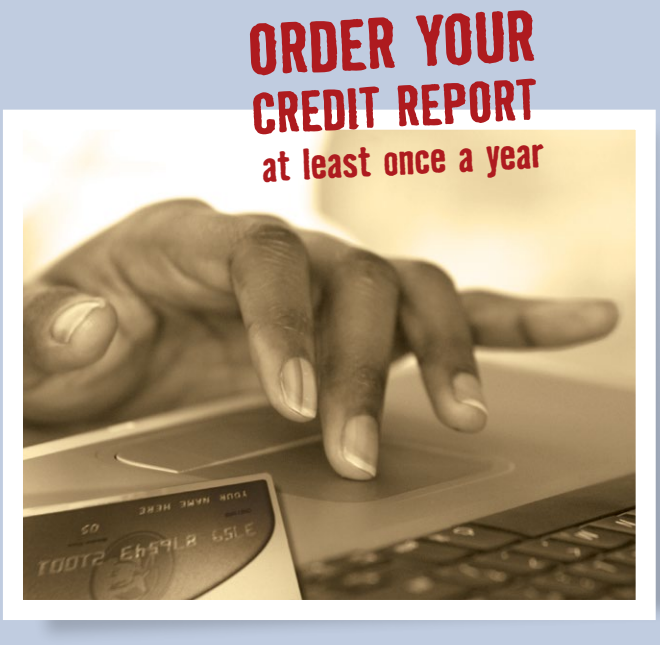
How Do I Know If I Am A Victim?

Here are some warning signs that you may be the victim of identity theft:

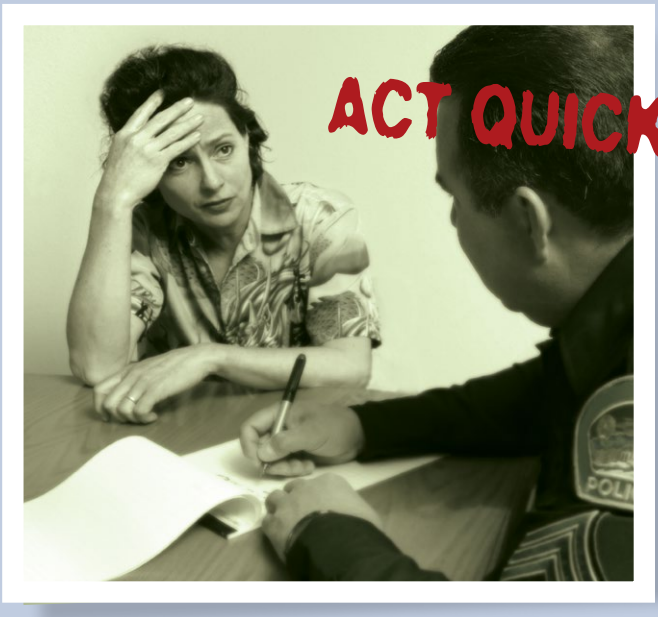
- You are denied credit;
- You find charges on your credit card that you don't remember making;
- Personal information, credit cards, ATM cards, checks or IDs have been stolen from you;
- You suspect someone has fraudulently changed your mailing address;
- Your credit card bills stop coming;
- You find something wrong on your credit report, such as loans you didn't take out or accounts you don't remember opening;
- A debt collector calls about a debt you didn't incur and didn't know about.

If any of these have happened, you may be the victim of identity theft.

You could be the victim of identity theft without noticing any of these things. It is good to keep a careful eye out for anything out of the ordinary by ordering your credit report at least once a year and being alert to these warning signs.



A free credit report is available
at www.annualcreditreport.com



File a police report

WHEN YOUR IDENTITY IS STOLEN

There are steps you will need to take to protect yourself. You may have to spend some time and money dealing with having your identity stolen.

You have to follow these steps without hesitation. Acting quickly is the best way to make sure this crime does not get out of control. The longer you wait, the more of your money someone else is spending and, potentially, the greater the damage to your credit.

Always remember to act quickly.

STEP 1: CONTACT THE POLICE

File a report with your local police department and, if the identity theft did not take place within your area, file a report with the police from the area where the theft took place. Make sure to get a copy of the police report. You may need that documentation to support your claims to credit bureaus, creditors, debt collectors or other companies. If you are unable to obtain a copy of the police report, be sure to get the report number.

STEP 2: CLOSING ACCOUNTS

If you notice any accounts under your name that have been tampered with or opened without your consent, close them immediately. The longer an identity thief has access to these accounts, the more money you could lose. Call each bank or company and then follow up in writing. If there are fraudulent charges or debts on your account or if a new account has been opened, you should immediately file a fraud report with your bank's fraud department. If a new account has been opened without your knowledge and consent, ask the company with which the account has been opened if they have a fraud department. If they do, file a fraud report with that department. If not, ask if they will accept the Identity Theft Affidavit from the Federal Trade Commission (see Step 5, page 16). If you close an existing bank account and open a new one, be sure to create new PINs (Personal Identification Numbers) and passwords.

STEP 3: FRAUD ALERT

The next step is to place a fraud alert on your credit file and carefully review your credit report. This will prevent an identity thief from opening any more accounts in your name. You should contact the three major credit bureaus listed on page 8. If you place a fraud alert with one credit bureau, that credit bureau is required by law to contact the other two bureaus. The other bureaus will include the fraud alert in their reports. However, to ensure that the alert is included in your credit file as quickly as possible to minimize potential damage to your credit history, contact all three credit bureaus immediately.

INITIAL FRAUD ALERT

Lasts at least 90 days.

Obtain an initial fraud alert when you suspect you might be a victim of identity theft, your wallet/purse is stolen or if you are a victim of "phishing." With an initial fraud alert, you are entitled to one free credit report from each credit bureau.

EXTENDED FRAUD ALERT

In your file for 7 years.

You can get an extended fraud alert on your credit report if you are a victim of identity theft and you have provided the credit bureau with an "Identity Theft Report." This type of fraud alert also entitles you to two free credit reports from each credit bureau within 12 months.

If you lose your Social Security card or think someone has it who should not, contact a credit bureau and have an initial fraud alert placed on your credit reports.

CREDIT BUREAUS

EQUIFAX
www.equifax.com

P.O. Box 740256
Atlanta, GA 30374-0241
888.766.0008

EXPERIAN
www.experian.com

P.O. Box 9532
Allen, TX 75013
888.EXPERIAN (397.3742)

TRANSUNION
www.transunion.com

P.O. Box 6790
Fullerton, CA 92834-6790
800.680.7289

After you have a fraud alert included in your credit history, you are entitled to receive a free copy of your credit report from each of the credit bureaus. Request a copy and review your report for these things:

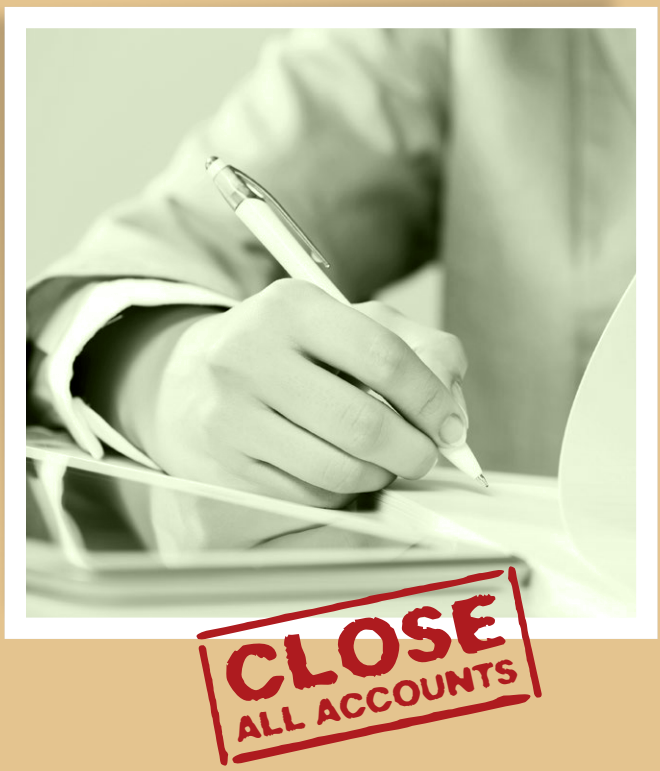
- Accounts you did not open;
- Debts on your account that you did not know about;
- Inquiries from companies you don't know;
- Inaccurate information.

CONSIDER PLACING A SECURITY FREEZE ON YOUR CREDIT REPORT

Arizona's security freeze law (ARS § 44-1698) allows a consumer to request that consumer credit reporting agencies place a security freeze on the consumer's credit report or consumer's credit score. The credit reporting agency must comply within ten business days of receiving a written request from the consumer and must provide the consumer with a unique ID number or password for the consumer to use to temporarily lift or permanently remove the security freeze.

Contact all three credit bureaus immediately

Can you believe this is happening?



STEP 4:
Fixing Specific Problems

You've identified the problems in your credit report, as well as identity theft problems elsewhere. Now it is time to fix them. Here's how:

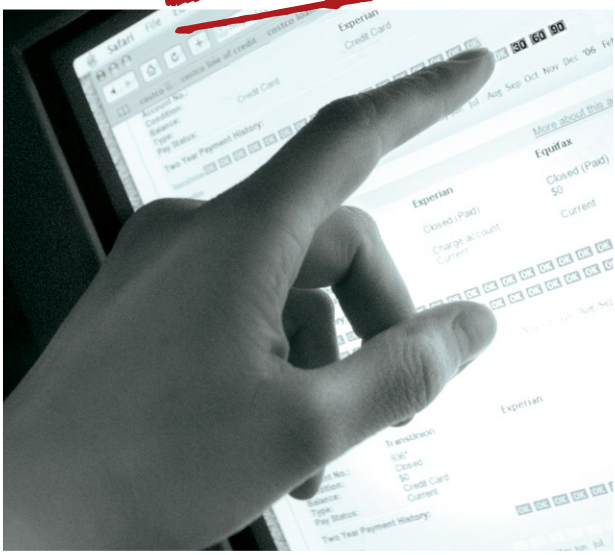
See CONTACTS on page 20 for contact information on these organizations.

EVENT	ACTION REQUIRED	CONTACT
You find any accounts tampered with or opened without your knowledge	Close the accounts immediately. Get new passwords and PINs for new accounts.	Credit bureaus and creditors (banks, credit card issuers)
Your ATM card, credit cards or checks were stolen	Close the accounts immediately. Get new PINs and passwords for new accounts. Notify each bank and major check verification companies. If your checks are stolen, put "stop-payments" on all checks remaining in the stolen checkbook. Ask any check verification company to put a fraud alert on your account.	Bank or credit card issuer, major check verification companies and the police
You find inquiries on your credit report that you did not know about	By phone and then in writing, notify the three major credit bureaus that unauthorized credit inquiries on your credit history were made and request that those inquiries be removed.	Credit bureaus
You find inaccurate information on your credit report	By phone and then in writing, notify the credit bureau of the incorrect information and request the information be corrected.	Credit bureaus
Healthcare Fraud / ID Theft	Contact healthcare provider Get medical records	Healthcare Provider

EVENT	ACTION REQUIRED	CONTACT
You have reason to believe your Social Security Number (SSN) has been stolen or misused	Report your allegations to the Social Security Administration, request a copy of your Social Security statement and/or call SSA to verify the accuracy of the earnings reported on your SSN.	Social Security Administration (SSA)
An identity thief has falsified change-of-address forms, stolen your mail or committed any other kind of mail fraud in order to get your personal information	Report it to your local post office. Contact your credit card companies, banks, etc. to notify them that your address was fraudulently changed.	U.S. Postal Inspection Service (USPIS)
You've lost your passport, it was stolen or you believe it is being misused	Contact the United States Department of State through a field office or on their website.	United States Department of State (USDS)
You think your name or SSN is being used to obtain a fraudulent driver's license	Contact the Motor Vehicle Division. Make sure you don't use your SSN as your driver's license number.	Motor Vehicle Division (MVD)
You think an identity thief has interfered with your security investments or a brokerage account	Report it to your broker or account manager as soon as possible. File a complaint with the U.S. Securities and Exchange Commission.	Your broker/account manager, U.S. Securities and Exchange Commission (SEC)

EVENT	ACTION REQUIRED	CONTACT
A phone service account has been opened in your name, someone is using your calling card or unauthorized calls are being billed to your cellular phone	Cancel your account and/or calling card. Use new PINs if you open new accounts.	Your service provider
A debt collector contacts you trying to collect on a loan that you did not take out	Write a letter to the debt collector. State your reasons why you dispute the debt and include supporting documentation, such as a copy of the police report or the FTC Identity Theft Affidavit.	Debt collector
You have been wrongfully accused of having committed a crime perpetrated by someone pretending to be you	File an impersonation report with the police, have your identity confirmed by providing documentation and prove your innocence by comparing your information to that of the identity thief.	You will possibly need the assistance of a criminal defense attorney (public or private) to clear your name. Contact the Public Defender's Office or the State Bar Association to find an attorney.
You believe someone has filed for bankruptcy in your name	Write to the U.S. Trustee and include supporting documentation. File a complaint with the U.S. Attorney and/or the FBI.	U.S. trustee in the region where the bankruptcy was filed, U.S. Attorney and FBI in the city the bankruptcy was filed. You may want to contact the Public Defender's Office or the State Bar Association to find an attorney to help you.

DON'T WAIT



You can check your credit report online immediately at www.annualcreditreport.com

FILE A COMPLAINT WITH THE FTC

Getting Your Credit Report Fixed

If you find inquiries on your credit report that you did not know about, contact the credit bureau and request that those inquiries be removed. If you find inaccurate information, contact the credit bureau to have it fixed. First call them and then follow up in writing. Provide copies of documents for support. If you cannot get any documentation from the creditor, send the credit bureau copies of your police report. Clearly identify what information you are disputing. Once your credit report is corrected, you can ask for the credit bureau to send notices of the corrections to anyone your credit report was sent to in the last six months.

Creditors

If your credit card was stolen or you find fraudulent charges on your credit card bill, close the account immediately. Then contact the credit card company about the fraudulent charges. Make sure your letter includes your account number and a description of the unauthorized charges, as well as your name and address. Send the creditor a copy of your police report and a copy of your Identity Theft Affidavit (see page 16). If they do not accept the Identity Theft Affidavit, fill out the creditor's fraud dispute forms. Request a return receipt so that you have proof of when the letter was received for your records, as well as to show that the letter arrived, within the required 60 days after you received the bill with fraudulent charges. Even if the address on your account was changed, you must still notify the creditor in writing within 60 days after the bill would have reached you. Remember to keep track of your billing statements. If you do not notify the creditor within 60 days, you may be liable for the fraudulent charges.

See Liability on page 19 for more information.

Social Security Number

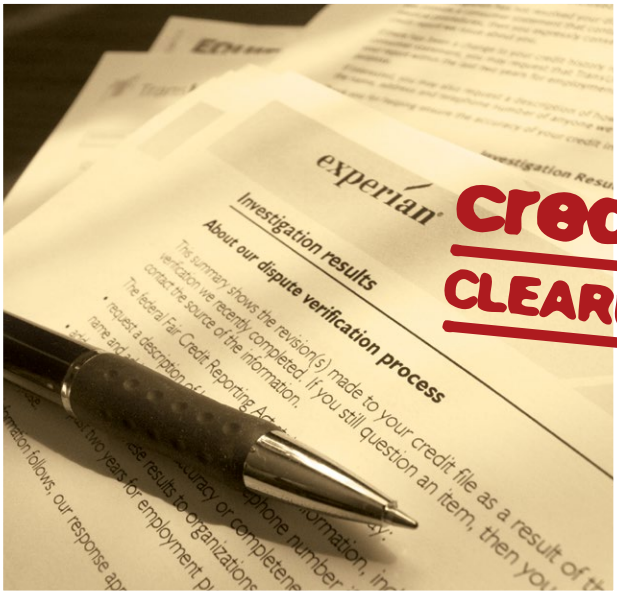
If you continue to have problems with an identity thief misusing your Social Security Number, the Social Security Administration (SSA) can issue you a new number, but this is not guaranteed to solve your problems. It is even possible that getting a new SSN will create more problems. A new SSN does not guarantee a new credit record. Credit bureaus might combine your new SSN credit record with your old SSN credit record. Even if that does not happen, the absence of any credit history might make it harder for you to get credit.

Also, you cannot get a new SSN if:

- You lost your SSN card or it was stolen but there is no evidence it is being misused;
- You filed for bankruptcy;
- You are planning on avoiding the law or legal responsibility.

the FASTER you act

THE LESS LIABLE YOU ARE



credit CLEARED

Criminal Violations

If an identity thief has impersonated you when they were arrested or cited for a crime, there are things you can do to correct your record. First, to prevent being wrongfully arrested, carry copies of documents showing that you are a victim of identity theft even if you do not know that criminal violations have been attributed to your name. If they have, contact the law enforcement agency (police or sheriff's department) that arrested the identity thief. Or if there is a warrant for arrest out for the impersonator, contact the court agency that issued it. You may also want to get a lawyer to help you.

STEP 5: Filing Complaints

The Federal Trade Commission (FTC) is the federal consumer protection agency. The FTC, in conjunction with the FBI, maintains an Identity Theft Data Clearinghouse. The FTC aids identity theft investigations by collecting complaints from identity theft victims and sharing the information with law enforcement agencies, credit bureaus, companies where the fraud took place and other government agencies. File a complaint with the FTC by going to *www.ftc.gov* or by calling their toll-free number at 877.ID.THEFT (877.438.4338).

Identity Theft Affidavit

A piece of documentation you need to fill out is the Identity Theft Affidavit offered by the Federal Trade Commission. This form will help you report information about your identity theft with just one form. Many companies accept this form, though others will require you to use their own form or submit more forms. If a new account has been opened in your name, you can use this form to provide the information that will help companies investigate the fraud. Once you have filled out the Identity Theft Affidavit as completely and accurately as possible, mail a copy to any of the companies concerned with the fraud you describe in the form, such as banks or creditors. The Identity Theft Affidavit, as well as more detailed information about filling it out, can be found at *www.ftc.gov.*

Make sure you keep copies of all your paperwork, including records of everyone you have corresponded with, fraudulent bills, police reports and complaint forms.

LIABILITY

To ensure that you don't end up paying hundreds or even thousands of dollars in fraudulent charges made by an identity thief, the best course of action is to act quickly. The faster you act, the less liable you are for unauthorized charges.

Credit Cards

According to the Truth in Lending Act, your liability is limited to $50 in unauthorized credit card charges per card in most cases. In order for this to come into effect, however, you must write to the creditor within 60 days of receiving the first bill that contained the fraudulent charge. If an identity thief changed your mailing address, you must still send your letter within 60 days of when you were supposed to have received it (keep track of your bills!).

ATM/Debit Cards

If your ATM or debit card is lost or stolen, report it as quickly as possible. If you report it within two business days, you are only responsible for $50 in unauthorized withdrawals or transfers. If you report it between two and 60 days after, you may be responsible for up to $500 in unauthorized withdrawals or transfers the thief may make. If you do not report it after 60 days, you can lose any money the thief withdraws or transfers from your account after the 60 days. Check your debit card issuer information. Some companies offer better protection when a card is stolen.

CHECKLISTS

Plan of Action List

Because this is a lot of information to take in, we have provided you with a checklist to make sure you have taken all the necessary steps after becoming an identity theft victim. Remember, you must complete all of these steps in a timely manner so that the identity theft does not get worse and to minimize your losses.

- [ ] 1. Filed a police report.
- [ ] 2. Call banks- CC/DC.
- [ ] 3. Obtained a copy of your credit report.
- [ ] 4. Identified errors, inquiries you did not know about, accounts you did not open, debts you did not know about or anything else that seems wrong or out of place on your credit report.
- [ ] 5. Placed a fraud alert on your credit report.
- [ ] 6. Closed any accounts that might have been tampered with or opened without your knowledge or consent.
- [ ] 7. Contacted a major credit bureau by phone and by writing to correct inaccurate information.
- [ ] 8. Filled out the FTC Identity Theft Affidavit.
- [ ] 9. Contacted the correct agencies to fix inaccurate information, close accounts or report identity theft.
- [ ] 10. Filed a complaint with the Federal Trade Commission.
- [ ] 11. Consider placing a security freeze on your credit report.

Document List

Here is a list of documents you should have. You won't be able to keep the originals of some of the documents, so it is very important that you keep copies.

It is also a good idea to keep copies of the documents that prove you are an identity theft victim with you, especially a copy of your police report.

- [ ] 1. Police report
- [ ] 2. Identity Theft Affidavit-FTC
- [ ] 3. Bills with fraudulent charges
- [ ] 4. Documentation of accounts opened in your name without your consent
- [ ] 5. Copies of letters sent to credit bureaus and creditors

CHILD IDENTITY THEFT

Child identity theft happens when someone uses a child's personal information to commit fraud. A thief may steal and use a child's information to get a job, government benefits, medical care, utilities, car loans, or even a mortgage. Studies show that children in the foster care system are more vulnerable to be victims of Identity Theft. Avoiding, discovering, and recovering from child identity theft involves some unique challenges and can be a lengthy process. Parents and guardians don't expect a minor child to have a credit file and rarely request or review their child's credit report because of believe in the child identity being safe and secure. A thief who steals a child's information may use it for many years before the crime is discovered, in many cases the child may not know until they are 18 years of age. An individual may not find out about the theft till years later, when applying for a job, loan, or apartment, or when a business reviews the credit file and finds fraudulent accounts. A parent or guardian can be proactive and check whether a minor child has a credit report if they think the child's information is at risk, say if the child's Social Security card was lost, a school or business leaked the child's personal information to the public, or bill collectors or government agencies contact the child about accounts the child didn't open. To get a minor child's credit report, a parent or guardian must contact the credit reporting companies and provide proof of identity and other documents.

How to find out if a child has a credit report

- ☐ **Contact each of the 3 nationwide credit reporting companies.**
  Email TransUnion: childidtheft@transunion.com.
  Call Experian (1-888-397-3742) and Equifax (1-800-525-6285).
- ☐ Ask for a manual search of the child's file.
  The companies will check for files relating to the child's name and Social Security number, and for files related only to the child's Social Security number.

  The credit reporting companies may require copies of:
  - *the child's birth certificate listing parents*
  - *the child's Social Security card*
  - *the parent or guardian's government-issued identification card, like a driver's license or military identification, or copies of documents proving the adult is the child's legal guardian*
  - *proof of address, like a utility bill, or credit card or insurance statement*
- ☐ **Update your files.**

PREVENTING ID THEFT IN THE FUTURE

No matter how many precautions you take, identity thieves can find a way to steal your identity. But there are ways to minimize your risk for identity theft and to help you recognize identity theft quickly.

1. **Place passwords on bank, credit card and phone accounts:** Don't use a password that could be easily guessed, such as your pet's name or your birth date, and choose a password that mixes random numbers with letters.

2. **Don't carry your Social Security Number card:** Don't even carry the number on you. Don't use it as your driver's license number. Keep the card in a safe place and use the number only when necessary.

3. **Order a copy of your credit report:** Order a copy from each of the three credit bureaus each year. A credit report contains information on where you live, where you work, how you pay your bills, whether you've ever been sued, arrested, or ever filed for bankruptcy, and what credit accounts have been opened in your name. Reviewing your credit report can alert you to any fraud or errors. This is very important and one of the best ways to catch identity theft. You are entitled to one free credit report annually from each of the three major credit reporting bureaus. Take advantage of it.

4. **Pay close attention to billing cycles:** If a bill does not arrive on time, it is possible that an identity thief may have taken it, so remember to check with creditors about a late bill.

5. **Guard your mail from theft:** Instead of leaving your mail to be picked up in an unlocked mailbox, take it to the post office or leave it in a post office collection box. Make sure you remove your incoming mail right away. Try not to leave mail in your mailbox overnight. Consider installing a mailbox with a lock.

6 **Don't give out personal information** over the Internet, on the phone or through the mail unless you have initiated contact with the receiving person or company or you are sure about the identity of the person or company. Be aware of schemes such as "phishing" in which the identity thief pretends to be from a legitimate organization or business in order to retrieve personal information from you. This might include calls or emails from someone claiming to be from your bank needing to confirm your Social Security Number or bank account number. Be aware of promotional scams that use phony offers as a way to obtain personal financial information.

7 **Keep your information safe online:** Only send your personal information, such as your credit card number, over a secure connection (a secure connection has an address that begins with "https" and has a small padlock at the bottom of the page; a window should also pop up telling you that the Web site is secure). Make sure you have virus protection that you update regularly. Use a firewall program to protect your computer from being accessed by others, especially if you have high-speed Internet which keeps your computer connected 24 hours a day, and a secure browser. You may also want to unplug your Internet while you are not using it. Don't download any files or click on links sent to you by people you don't know.

8 **Take advantage of security features that can add an extra layer of protection.** Protect home computers and laptops by installing and using virus, malware and spyware software, including those programs that provide protection against, detection of and removal of keyloggers. Computer hackers can gain access to Personal Identifying Information through various methods that track the passwords and other information you type on your computers.

Ask your financial institution what security features they offer and choose which ones are best for you. These can be particularly important if you or someone you love suffers from dementia or other debilitating health problems, or if there is potential for care givers or others to gain access to financial information. Many institutions offer an array of valuable protections for vulnerable consumers, including:

- Fixed limits on savings and checking withdrawal
- Delaying or declining transactions that exceed predetermined limits or appear suspicious;
- Notifying a designated third party of any suspicious transactions;
- Preventing or limiting electronic account access;
- Formal bank protocols for monitoring and reporting suspected financial abuse or exploitation.

9 **Carefully analyze identity theft protection services** before purchasing. Identity theft protection services such as credit-report monitoring, fraud alerts, identity theft insurance and help for victims of identity theft are all available for a fee. Some credit restoration services are very expensive. Most of the companies offer a package of services that can give peace of mind in restoring credit. However, you can do much of what these services provide for free. If you decide to use a service, make sure to do your research before selecting one. The Attorney General's Office cannot vouch for the reliability or quality of any specific services or products, so be sure to check the track record of companies with the Better Business Bureau.

10 **Consider placing a Security Freeze on your Credit Report.** Arizona's security freeze law (ARS § 44-1698) allows a consumer to request that consumer credit reporting agencies place a security freeze on the consumer's credit report or consumer's credit score. The credit reporting agency must comply within ten business days of receiving a written request from the consumer and must provide the consumer with a unique ID number or password for the consumer to use to temporarily lift or permanently remove the security freeze.

CONTACTS

Arizona Attorney General's Office

www.azag.gov

Crime and Fraud Prevention Program
1275 West Washington Street
Phoenix, AZ 85007

Identity Theft Help Line
602.542.2145 (Phoenix)
520.628.6504 (Tucson)
800.352.8431 (Outside Maricopa and Pima Counties)
identitytheft@azag.gov

Satellite Office locations throughout the state
800.352.8431 (outside Phoenix and Tucson)

Arizona Department of Transportation Motor Vehicle Division

www.azdot.gov/mvd

602.255.0072 (Phoenix)
520.629.9808 (Tucson)
800.251.5866 (outside Phoenix and Tucson)

Remove your Social Security Number from your driver's license or order a duplicate driver's license at *www.servicearizona.com*

Credit Reports

If your personal information is stolen or you notice any suspicious activity involving your credit, immediately contact one of the credit reporting bureaus and ask them to place a Fraud Alert on your accounts:

Equifax

www.equifax.com

P.O. Box 740256
Atlanta, GA 30374-0241
888.766.0008

Experian

www.experian.com

P.O. Box 9532
Allen,TX 75013
888.397.3742

TransUnion

www.transunion.com

P.O. Box 6790
Fullerton, CA 92834-6790
800.680.7289

Remove your name from credit bureau mailing lists or pre-approved, unsolicited credit and insurance offers by calling 888.567.8688 (888.5OPTOUT) or online at *www.optoutprescreen.com*

Order your free credit report

Take advantage of your free annual credit reports, now a requirement of federal law. You are eligible to receive a free credit report from each of the three credit reporting bureaus every year. Ordering a report from one of the bureaus every four months allows you to check your credit report three times a year for free.

To order your **free credit report**, call 877.322.8228, request it at the central Web site established by the three credit bureaus, *www.annualcreditreport.com*, or complete the Annual Credit Report Request Form and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The request form is available on the FTC Web site at *www.ftc.gov.*

TDD 877.730.4104

Check Verification Companies

If an identity thief steals your checks or creates counterfeit checks from your existing bank account, stop payment, close the account and ask your bank to notify the check verification service with which it does business. That way, retailers can be notified not to accept these checks. You can contact major check verification companies directly to request that they notify retailers who use their databases not to accept your checks:

Chexsystems

www.chexhelp.com

Attention: Consumer Relations
7805 Hudson Road, Suite 100
Woodbury, MN 55125
800.428.9623

TeleCheck Services, Inc.

www.telecheck.com

TRS Recovery Services, Inc.
Attention: Forgery Department
P.O. Box 4451
Houston, TX 77210-4451
800.366.2425

Certegy Check Services, Inc.

www.certegy.com

P.O. Box 30046
Tampa, FL 33630
800.770.3792

consumer.inquire@certegy.com
To find out if the identity thief has been passing bad checks in your name, call SCAN at 800.262.7771

Federal Agencies

Federal Bureau of Investigations (FBI)

www.fbi.gov

J Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, DC 20535-0001
202.324.3000 (false civil and criminal judgments)

Federal Trade Commission (FTC)

www.ftc.gov

Identity Theft Clearinghouse
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
877.438.4338 (ID Theft Hotline)
TTY 866.653.4261

Telemarketing

To remove your name and home address from national telemarketing mailing and phone lists, visit the consumer page at *www.the-dma.org*. The Federal Trade Commission's (FTC) Do Not Call Registry allows you to stop getting telemarketing calls at home. You can register either online at *www.donotcall.gov* or by calling 888.382.1222 (TTY 866.290.4236) toll free from the number you wish to register.

Do Not Call Registration is free. If you receive a call after your phone number has been on the registry for 31 days, contact the FTC (see above listing) and report the company. Some callers are not subject to Do Not Call (former business relationships within the last 18 months, charitable solicitations and political calls). A complete list of exceptions can be found on the Arizona Secretary of State's Web site at *www.azsos.gov.*

Internal Revenue Service (IRS)

www.irs.gov

Fresno, CA 93888
800.829.0433 (tax fraud hotline)

Securities and Exchange Commission (SEC)

www.sec.gov

SEC Complaint Center
100 F Street NE
Washington, DC 20549-0213
800.732.0330

Social Security Administration (SSA)

Office of the Inspector General

www.ssa.gov

Social Security Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235
800.269.0271
TTY 866.501.2101

U.S. Passport Agency

www.travel.state.gov

1111 19th Street, NW
Washington, DC 20522-1705
877.487.2778

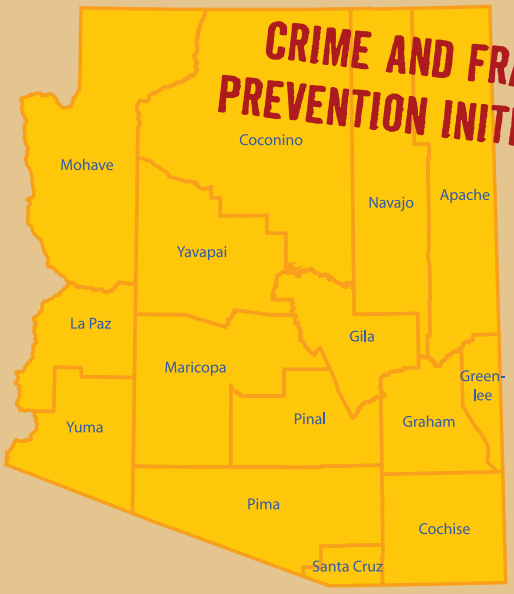
If you are a victim of identity theft and the U.S. Mail is involved, call your nearest Postal Inspection Service office. You can also report identity theft involving the U.S. Mail online.

U.S. Postal Inspection Service (USPIS)

www.usps.com/postalinspectors

P.O. Box 20666
Phoenix, AZ 85036-0666
877.876.2455

CRIME AND FRAUD PREVENTION INITIATIVES



The Arizona Attorney General's Community Outreach & Education Division is committed to educating Arizona residents about crime prevention, identity theft, civil rights, internet safety, consumer fraud, senior abuse and victims rights. Community Outreach Coordinators are available, statewide, to give educational presentations to community groups, schools, senior centers and veteran's groups; additionally we are available to distribute educational materials at local events. Our office operates a network of satellite offices, staffed by volunteers, throughout the state making it easier for Arizona residents to gather information and remain educated about the issues affecting them. Our goal is simple: to prevent YOU from becoming a victim. A complete list of satellite offices, upcoming events and information about requesting presentations is available on the Attorney General's website ***www.azag.gov***.

ARIZONA ATTORNEY GENERAL
MARK BRNOVICH
DEFENDING ARIZONA

For more information, contact:

Community Services Program
Arizona Attorney General's Office
1275 West Washington Street
Phoenix, Arizona 85007
602.542.2123 or 1.800.352.8431
communityservices@azag.gov

Subscribe to the Attorney General's consumer alerts and messages on current issues at *www.azag.gov.*

Publications available from the Arizona Attorney General's Office include:

- Top Consumer Scams
- Civil Rights:
  - Employment Discrimination
  - Discrimination in Places of Public Accommodation
  - Housing Discrimination
  - Voting Discrimination
- Identity Theft Guide
- Internet Safety
- Life Care Planning

ACTIVE DUTY ALERTS FOR MILITARY PERSONNEL

Military personnel have additional protections. If you're deployed, you can place an active duty alert on your credit reports to help minimize the risk of identity theft while you're away. Active duty alerts last for 1 year. If your deployment lasts longer, renew the alert.

How to request an active duty alert

☐ **Contact 1 credit reporting company.**

Equifax
1-800-525-6285
Experian
1-888-397-3742
TransUnion
1-800-680-7289

☐ Request an active duty alert.

☐ Provide proof of identity, like a government-issued identity card, driver's license, military identification, birth certificate, or passport.

The company you call must contact the others.

The credit reporting companies will take your name off their marketing list for prescreened credit card offers for 2 years, unless you ask them to add you back onto the list.

☐ **Mark your calendar.**

Active duty alerts last for 1 year. If your deployment lasts longer, renew the alert.

☐ **Update your files.**

RESPOND QUICKLY TO NOTICES FROM THE INTERNAL REVENUE SERVICE

If you get a notice from the IRS that suggests someone misused your Social Security number, respond quickly to the address included with the notice. It is important that I you are a service member you make someone aware to inform you weather you receive a notice in the mail regarding the IRS. The notice may say that you didn't pay taxes on a job you know you never held, or that your Social Security number was used on another return. Remember that the IRS never makes first contact with taxpayers by email, and doesn't ask for personal information through email. If you get email that claims to be from the IRS, call the IRS before you respond. Call 1-800-829-1040 for more information.

If you find out that an identity thief has used your Social Security number on a tax return, call the IRS's Specialized Identity Theft Protection Unit at 1-800-908-4490.

ARIZONA ATTORNEY GENERAL'S OFFICE | www.azag.gov | communityservices@azag.gov

Phoenix 602.542.2123 | 800.352.8431 (outside Phoenix and Tucson)

Arizona Attorney General's Office

1275 West Washington Street
Phoenix, Arizona 85007

400 West Congress, South Building
Suite 315
Tucson, Arizona 85701

WE ARE HERE TO
HELP YOU!