ATTORNEY GENERAL
LESLIE RUTLEDGE
ARKANSASAG.GOV

Identity Theft

Identity theft occurs when someone uses your personal information without your permission to commit fraud — most commonly to obtain access to credit in your name. Personal information:

- Social Security number
- Driver's license number
- Bank account number
- Credit card number
- Personal Identification Numbers (PINs)
- Mother's maiden name or other information used as a security screen
- Passwords
- Any other piece of key information that can be used to gain access to a person's financial resources or to assume a person's identity

<u>Minimize Risks</u>

- Mail bills from a secure location and don't leave sensitive mail in your mailbox for extended periods.

- Shred or destroy statements, documents or records that contain personal or financial information after they are no longer needed.

- The most common form of identity theft is through lost or stolen documents, checkbooks or credit cards. Don't carry information you don't need in your purse or wallet, Social Security card unless you need it that day and PINs attached to credit, debit or ATM cards.

- Store financial records and important information in a safe place in your home.

- Beware of giving personal information over the phone. Know who you are dealing with. When in doubt, hang up and get the business or government agency's number from an independent source.

- Use anti-virus and anti-spyware software, as well as a firewall, and regularly update.
  - Properly set up operating system and web browser software and regularly update.

- Avoid passwords like your birth date, spouse or child's name or birth date, mother's maiden name or the last four digits of your Social Security number.

- Don't share personal information over the internet.
  - Never respond to an email that asks you to transmit personal information online. Legitimate companies will not make such requests.
  - Your bank or credit card issuers already have your account numbers, PINs, access codes, passwords, Social Security number and other information they need. They won't email you to ask for it.

- For tips about protecting yourself from internet fraud and securing your computer, visit **onguardonline.gov**.

How Can I Tell If My Identity Has Been Stolen?

- Review bank, credit card and financial account statements for unusual activity. Promptly report unauthorized charges to the account provider.

- Check your credit report at least once a year for accuracy and to determine whether accounts have been opened in your name without your knowledge
  - Everyone is allowed one free credit report a year from each of the three national credit bureaus.
  - You have the right to have inaccurate or outdated entries removed from your report.
  - To learn how to obtain your free credit report, visit **annualcreditreport.com**.

<u>Red Flags</u>
- Getting an account statement or collection calls regarding an account you did not authorize
- If your monthly credit card statement stops coming to your address
- Having a credit application denied when you don't believe you have a credit history problem
  - Periodically review your credit report and review it before you apply for credit on a large purchase.

What Should I Do if I'm a Victim of Identity Theft?

The Attorney General's office recommends taking the following steps as soon as possible:

1. File an identity theft **report** with your local **law enforcement** agency.

2. File a **fraud alert**, statement on a credit bureau report to help consumers who may have been a victim of identity theft, with one of the three national credit bureaus.
   - A fraud alert is intended to stop an identity thief from using your personal information to open fraudulent credit accounts in your name.
   - When a creditor or business reviews a credit report in which a fraud alert has been placed, they verify the applicant's identity and may contact you. Make sure your contact information is current on your credit report.

- An **initial fraud alert**, which covers 90 days, is appropriate if your wallet has been stolen or if you suspect your identity has been or will be compromised.
  - You will be entitled to one free credit report from each of the three nationwide credit bureaus.

- An **extended fraud alert**, which lasts seven years, is for a consumer who knows that he or she is a victim of identity theft.
  - You will be required to provide the credit bureau with a copy of an identity theft report, such as a police report, and appropriate proof of your identity.
  - You will be entitled to two free credit reports within 12 months from each of the credit bureaus.
  - The consumer reporting companies will remove your name from marketing lists for prescreened credit offers for five years unless you ask to add your name back.

- To place or rescind a fraud alert, contact one of the credit bureaus, which are required to share fraud alert requests with the other bureaus, and provide proof of your identity.

3. **Close accounts** that have been tampered with or opened fraudulently.
   - It is imperative that you contact the company involved to dispute the fraudulent transactions or accounts.
   - Follow up with the company in writing. Sending correspondence by certified mail is recommended.
   - Ask the company whether a fraud affidavit is required. If it is, the company may send you its affidavit, or you can get one from the Federal Trade Commission's identity theft booklet, which is also available from the Attorney General's office.

4. File an identity theft **complaint** with the **Federal Trade Commission: ftccomplaintassistant.gov** or call (877) IDTHEFT (438-4338).

5. Consider requesting an **Identity Theft Passport** provided by the Arkansas Attorney General's Office.

6. Consider placing a **security freeze** on your credit report.
   - Any person, whether victim of identity theft or not, may place a security freeze to prohibit a consumer reporting agency from releasing information in your credit report without your authorization.
     - It is intended to prevent credit, loans and services from being approved in your name without your consent.

- Using a security freeze may delay or prevent prompt approval of subsequent applications regarding a new loan, credit, mortgage, government service or payment, rental housing, employment, investment, license, phone, utilities, digital signature, internet credit card transaction, or other services, including an extension of credit.

- When you place a security freeze, you will be given a personal identification number or password.

- To remove the security freeze or authorize the release of your credit report, contact the credit bureau and provide:
  - Personal identification number or password
  - Proper identification to verify your identity
  - Time period for which the credit report shall be available

- The national credit bureau must authorize the release of your credit report for a period of time within 15 minutes or as soon as practical if good cause exists for the delay and must remove a security freeze no later than three business days after receiving all of the above items by any method the consumer reporting agency allows.

- A security freeze does not stop all access to your credit report. Companies with which you have an existing account or collection agencies acting on behalf of such companies may request information from your credit report.
  - Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.
  - You have the right to bring a civil action against anyone including a national credit bureau that willfully or negligently fails to comply with any requirement of the Arkansas Consumer Report Security Freeze Act.

- A credit bureau can charge you up to $5 to place, temporarily lift or remove a security freeze.
  - However, you should not be charged if you are 65 or older or if you are a victim of identity theft and have submitted, in conjunction with the security freeze, a copy of a valid investigative or incident report.

Consumers may request a security freeze by one of the following:

1. Send request in writing by mail to a national credit bureau.
2. Call credit bureau and provide proper identification information.
3. Electronically forward request to a credit bureau through a secure connection if it is available by the national credit bureau.

Credit reporting agencies

Equifax
equifax.com
(800) 525-6285
P.O. Box 740241
Atlanta, GA 30374- 0241

Experian
experian.com
(888) 397-3742
P.O. Box 9554
Allen, TX 75013

TransUnion
transunion.com
(800) 680-7289
Fraud Victim Assistance Division, P.O. Box 2000
Chester, PA 19016