MOUNTAIN VIEW POLICE DEPARTMENT

GEORGE BETHELL
CHIEF OF POLICE

203 South Peabody Avenue | P.O. Box 1048 | Mtn. View, AR 72560
Phone (870) 269-4211 | Fax: (870) 269-5868

This information has been obtained directly from the Arkansas Attorney Generals Office webpage located at https://arkansasag.gov/

IDENTITY

Identity theft is a crime that occurs when someone uses your personal information without your permission to commit fraud or other crimes — most commonly to obtain access to credit in your name. Personal information includes:

- Social Security, driver's license and personal identification numbers
- Bank and credit card account numbers
- Mother's maiden name or other information used as a security screen
- Passwords and any information that can be used to gain access to a person's financial resources or to assume a person's identity

Identity theft can happen by:

- **Mail** — Looking for red flag up on mailboxes and bill payments
- **Trash** — Digging for discarded receipts, credit card, and bank account statements, credit card applications, etc.
- **Home** — Stealing important documents, such as credit card and bank account statements, checkbooks, Social Security cards, drivers' licenses, and birth certificates
- **Computers** — Illegally gaining access to computers to steal your personal information, such as following financial transactions
- **Businesses** — Bribing employees who have access to personal information at businesses or data breaches
- **Email phishing** — Posing as a legitimate company, emails request verification of personal information
- **Phone pretexting** — Calling and posing as a legitimate company, requesting you verify personal information, or they may contact an information source, posing as you, seeking personal information
- **Wallet or purse**
- **Relatives and friends**

HOW CAN I PROTECT MYSELF

Although there is no way to make sure that your personal information is totally safe, you can take steps to avoid becoming a victim.
Minimize risks:

- Mail your bills from a secure location and do not leave sensitive mail sitting in your mailbox for extended periods.
- Shred or otherwise destroy any statements, documents, or records which contain personal or financial information after they are no longer needed.
- The most common form of identity theft continues to be obtaining personal information through lost or stolen documents, checkbooks, or credit cards.
    - Do not carry:
- Store important information in a safe place in your home. Do not leave financial records lying around your house.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them regularly.
    - Set up your operating system and web browser software properly, and update them regularly.
- Avoid using 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.
- For tips from the federal government and the technology industry about protecting yourself from internet fraud and securing your computer, visit OnGuardOnline.gov.
- Do not share personal information over the internet.
    - Don't get reeled in by a phishing scam. 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.
- 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.

How can I tell If my identity has been stolen?

Due diligence is the best way to detect suspicious activity that may be the result of identity theft.

- 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.
    - Everyone is allowed one free credit report per year from each of the three national credit bureaus: Equifax, Experian, and TransUnion.
    - By checking your credit report you can determine whether accounts have been opened in your name without your knowledge.
    - Also, you can check the accuracy of the report. You have the right to have inaccurate or outdated entries removed from your credit report.
    - To learn how to obtain your free credit report, please visit AnnualCreditReport.com.

Red flags

- Getting an account statement for an account that you did not authorize is an indication that you may be the victim of identity theft. Likewise, getting collection calls from a creditor or debt collector regarding an account that you did not authorize is an indication that you may be the victim of identity theft.
- Not receiving expected bills or account statements. If your monthly credit card statement stops coming to your address, this could be an indication that someone has stolen your mail or changed your account statement mailing address. Promptly report this to the account provider.
- Having a credit application denied when you have no reason to believe you have a problem with your credit history. Be sure to periodically review your credit report, and always review it again before you make an application for credit on a big purchase.

WHAT SHOULD VICTIMS DO

If you believe you are a victim of identity theft, we urge you to take the following steps as soon as possible:

- File a **fraud alert** with one of the three national credit bureaus.
- File an identity theft **report** with your local **law enforcement** agency.
- **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.
- File an identity theft complaint with the **Federal Trade Commission** or call (877) IDTHEFT (438-4338).

- Consider placing a **security freeze** on your credit report.
- Consider requesting an identity theft passport provided by the Attorney General's office.

Identity Theft Passport

In 2005, the Arkansas Legislature approved Act 744, which gives the Attorney General authority to issue an identity theft passport to an Arkansas resident who learns or reasonably suspects that he or she is a victim of financial identity fraud and who has filed a police report.

The identity theft passport is a card, similar in appearance to a driver's license, is designed to assist financial identity fraud victims in re-establishing their good names. This passport may also help prevent a victim's arrest for other criminal offenses committed by the identity thief.

FRAUD ALERT/SECURITY FREEZE

Fraud Alert
A fraud alert is a statement on a credit bureau report to help consumers who may have been a victim of identity theft.

- 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.

Security Freeze

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.

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

SECURITY OR DATA BREACH

A security breach or data breach is one of the most common causes of the disclosure of personal information. These breaches can expose the personal information of a few thousands, or even millions of individuals. It occurs when personal or otherwise sensitive information that is maintained by an entity is accessed in an unauthorized manner or when that information is inadvertently exposed. Such an incident certainly increases one's risk of identity theft. However, it should be noted that not all personal information compromises result in identity theft.

The Arkansas Personal Information Protection Act requires entities that collect personal information to use reasonable security procedures and practices to protect such information. Additionally, the law mandates that in the event such information is compromised, the entity must notify the affected individuals in a timely manner. Notification to individuals whose personal information has been compromised allows them to take steps to mitigate the potential misuse of their information.

The Arkansas Personal Information Protection Act was recently amended to require that a breach be reported to the Arkansas Attorney General if the breach affects the personal information of more than 1,000 individuals and the reporting entity determines that there is a reasonable likelihood of harm to consumers.

THIS ONLINE FORM MAY BE USED TO REPORT A DATA BREACH.

Although it is not required by Arkansas law, many businesses that experience a security breach will offer credit monitoring services at no charge to affected individuals usually for one year. Credit monitoring can be useful in this context; however, it is entirely up to the consumer whether he or she wants to take advantage of such an offer.

What should I do if I receive a security breach notification?

- If the compromised information relates to existing financial accounts, contact your financial institution to close or change the account information as soon as possible.
- Consider placing a fraud alert on your credit bureau reports.

- Consider placing a security freeze on your credit bureau reports.
- Periodically monitor your credit bureau reports for any unusual activity and check for accuracy. Everyone is allowed one free credit report per year from each of the three major credit bureaus. To learn how to obtain your free annual credit report under federal law, visit AnnualCreditReport.com or call (877) 322-8228. A victim of fraud is eligible to receive one free credit report from each of the major credit bureaus. Requests for a free report based on a fraud claim should be made directly to the credit bureaus:
    - TransUnion LLC: (800) 916-8800; TransUnion.com; P.O. Box 2000, Chester, PA 19016
    - Experian: (866) 200-6020; Experian.com; P.O. Box 2002, Allen, TX 75013
    - Equifax: (888) 766-0008; Equifax.com; P.O. Box 740241, Atlanta, GA 30374