Important Information on Identity Theft

Auburn Banking Company is committed to customer education and prevention of Identity Theft. As part of this ongoing effort, we have compiled a list of frequently asked questions and helpful tips to prevent our customers from falling victim to identity thieves. Please take a moment to read this important document. The steps you take now to insure the safety of your personal information could make the difference tomorrow. As always, if you have any questions, please call us at either location or visit us on the web at www.auburnbankingcompany.com for more information about identity theft.

What is Identity Theft? Identity theft is the unlawful use of another person's identification. Identity theft may take many forms. Common methods of identity theft include credit card or other financial institution fraud, phone or utility service theft, insurance identity theft, medical identity theft, criminal identity theft, and tax identity theft. However, thieves are finding new ways of using the identity of their victims every day. One way in which our financial institution can help protect your account information from thieves and unauthorized users is to educate you on identity theft**.**

How does Identity Theft Occur? Surprising to most people is that identity theft is actually a very easy crime to commit. In fact, according to Javelin Strategy and Research's 2017 report, there were 16.7 million victims of identity theft in 2017 alone. That being the case, it is important for you to know how these thieves operate so you can protect your personal information. At the heart of the crime is the thief obtaining information that most people would assume only the true owner of the information would know. Common examples are social security numbers, driver's license numbers, mother's maiden names, and passports. Thieves obtain this information in numerous ways. Some thieves will steal wallets, purses, mobile devices, and even mail. Others will listen and/or watch a person conduct personal business, such as an automated teller machine. Thieves will also deceive or trick people into disclosing personal information through phone scams, via the mail, on the Internet, or through mobile applications "apps". Very aggressive thieves will even obtain personal information by using a process referred to as "pretext calling." Pretext calling occurs when an individual contacts an entity in possession of a customer's personal information and cons the entity into releasing the information by acting as the customer or someone authorized to have the customer's information. Once a thief has possession of the information, the thief will apply for credit cards, loans, phone services, or just about any other service where economic gain can be realized without actual payment. When applying for credit cards, loans, or other services, thieves will often intentionally use incorrect addresses or complete change of address forms on existing accounts so that the victim will not be immediately aware of the crime.

How Does Identity Theft Affect Me? Identity theft can cause its victims numerous problems. Most significantly, it can destroy the financial history you have worked so hard to obtain. Repairing your credit history can require significant time and money. You may not be able to stop a thief until thousands of dollars of debt have been attributed to you.

How Can I Protect Myself From Identity Theft? The following are just some of the ways you can reduce the risk of identity theft:

- Keep your credit cards, debit cards, personal identification numbers (PINs) and other passwords, checks, social security cards, other cards or documents which bear your social security number, health insurance cards, driver's license and number, and other personal information where they will be safe. When disposing of these items, do so by shredding.
- Keep your deposit and withdrawal slips, credit card purchase receipts, financial institution statements, credit card statements, utility bills, medical bills, insurance information, investment updates, and credit card solicitations where they will be safe. When disposing of them, do so by shredding.
- Install antivirus and antimalware software on home computers.
- Enable security features on mobile devices especially if you have contacts, banking websites, and "apps" saved.
- Don't put your trash out until shortly before it will be picked up.
- Mail bill payments and other items that contain personal information at a U.S. Postal Service drop box rather than in your curb side mailbox. Don't put any mail in your curb side mailbox until shortly before it will be picked up.
- Take your mail out of your curb side mailbox as soon as possible after it has been delivered. If you are traveling, have the U.S. Postal Service hold your mail or have someone you trust pick it up daily.
- Limit the information on your checks, and don't carry around any more cards than necessary.
- Don't give any of your personal information in person, over the telephone, or over the Internet to anyone unless you have a very good reason to trust them.
- Don't reply to or click on any links in suspicious emails, texts, or social media messages.
- Don't give any of your personal information to any web sites that do not use encryption or other secure methods to protect it. (Look for sites starting with URL https://, meaning it is a secure site.)
- Use a firewall if you have a high-speed Internet connection. This software can be purchased online or from most software retailers. Also, install and keep antivirus and anti-spyware software up to date.
- Don't use PINs or passwords that are easy to guess (for example, don't use birth dates, or spouse, child or pet names).
- Do not access mobile banking via public Wi-Fi, or other "apps" in which you have confidential information stored.
- Create complex passwords that identity thieves cannot guess easily.

- Examine your credit card and financial institution statements immediately upon receipt to determine whether there were any unauthorized transactions. Report any that you find immediately to the financial institution.
- Make a prompt inquiry if bills or statements are not received in a timely fashion - this could mean that they are being diverted by an identity theft.
- File income taxes early in the season, before a thief can file taxes in your name.
- Review explanation of benefits medical summary notices to make sure that medical claims being filed match services rendered.

You may also wish to do the following:

- Obtain copies of your credit report annually from each of the three major credit reporting agencies to be sure that they are accurate.
- Request a credit freeze with the three major credit bureau reporting agencies.
- Request not to receive any further pre-approved offers of credit by calling 1-888-5-OPT-OUT.
- Register with the National Do Not Call Registry by calling 1-888-382-1222 or going online at www.donotcall.gov.
- Ask to be removed from national direct mailing lists by writing to: DMA Mail Preference Service; P.O. Box 643; Carmel, NY 10512

How Can I Monitor My Credit Report Activity? You are allowed to get one free credit report each year from each of the three major credit bureaus listed below. After getting your credit report, look for warning signs of actual or potential identity theft. Warning signs can include credit opened in your name that you did not apply for or a request for a copy of your credit report when you did not request it.

What Should I Do If My Identity Has Been Stolen? In the event that you suspect your identity has been stolen or you are, in fact, certain that it has been stolen, follow these simple steps:

1. Contact the fraud department of at least one of the following three major credit reporting agencies and ask that a fraud alert be placed in your credit file and for a free credit report (to be on the safe side you may wish to contact all three):

EQUIFAX
1-888-766-0008
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

EXPERIAN
1-888-EXPERIAN (1-888-397-3742)
P.O. Box 9532
Allen, TX 75013
www.experian.com

TRANSUNION
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

2. Close all accounts that are or may be affected by the identity theft. Also, regarding any checking accounts thus closed, contact the following major check verification companies and ask that retailers using their databases not accept checks drawn on the closed accounts:

- **TeleCheck - 1-800-710-9898 or 1-800-927-0188**
- **Certegy, Inc. - 1-800-437-5120**
- **International Check Services - 1-800-631-9656**

3. File a police report and obtain a copy for submission to credit reporting agencies, creditors, and others.

4. Contact the Federal Trade Commission to report the theft and obtain further guidance as to how to protect yourself:

- Website: www.ftc.gov or IdentityTheft.gov
- Call: 1-877-IDTHEFT (438-4338)
- Write: Federal Trade Commission
  Consumer Response Center
  600 Pennsylvania Avenue, NW
  Washington, DC 20580

5. If you know or suspect that your mail has been stolen, contact the United States Postal Service.

6. Keep detailed records of any theft of your identity and of your efforts to resolve the same.