AUBURNBANK

Member FDIC | AuburnBank.com

External Website Disclaimer - At certain places on our Website, there are links to other Websites. AuburnBank does not endorse, approve, certify, or control those external sites and does not guarantee the accuracy, completeness, efficiency, timeliness, or accurate sequencing of the information contained in them.

IDENTITY THEFT: Steps to take if you are a Victim

If you suspect misuse of your personal information to commit fraud, take action immediately. Keep a record of all conversations and correspondence when you take the following suggested steps:

1) **Contact your bank(s) & credit card issuers immediately.**

2) **File a police report with your local police department.**

3) **Contact the three major credit bureaus.**
   a. Equifax 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30274-0241
   b. Experian 1-888-397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013
   c. TransUnion 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

4) File a complaint with the Federal Trade Commission.
   a. 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 identity thieves and stop them.
   b. You can file a complaint online at www.ftc.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission 600 Pennsylvania Avenue, NW, Washington, DC 20580.

To help protect from identity theft:

- Photocopy contents of your wallet, keep in a secure place.
- Keep your checks in a secure area.
- Review your bank statements immediately upon receipt.
- Do not list Social Security Number, Driver's License Number or Date-Of-Birth on your checks.
- May use P.O. Box as your address on your checks.
- Shred or burn all sensitive documentation or mailings. Do not throw them into the trash.
- Put outgoing mail into a secure, official Postal Service collection box.
- Do not leave wallet or purse in auto unattended, including the trunk of your vehicle.
- Sign new credit cards immediately.
- Memorize your Social Security number and passwords.
- Don't use your date of birth as your password and don't record passwords on papers you carry with you.
- Beware of mail, e-mail or telephone solicitations that offer prizes or awards--especially if your personal information or financial account numbers are requested.

5) **If your Social Security Number was compromised** contact Social Security Administration Fraud Hot Line at 1-800-2690271.

6) **If you are a victim of an internet scam please notify the Internet Crime Complaint Center by filing a report at www.ic3.gov.** IC3 gives details of the following types of internet fraud; Auction, Counterfeit Cashier Check, Credit Card, Debit Elimination, DHL/UPS fraud, business or employment opportunities, escrow service fraud, identity theft, internet extortion, investment fraud, lotteries, Nigerian Letters or “419” fraud, Phishing/Spoofing, Ponzi/Pyramid fraud, reshipping, spam, third party receiver of funds fraud.

7) **If you believe you’re a victim of fraud related to the U.S. Mail,** including mailed sweepstakes, lotteries, on-line auctions, Work-at-home scams, secret shopper surveys or chain letters, report your concern to the U.S. Postal Inspection Service. https://postalinspectors.uspis.gov/

8) **If you believe you’re a victim of fraud that was received by UPS (United Parcel Service)** including mailed sweepstakes, lotteries, on-line auctions, work-at-home scams, secret shopper surveys, fraudulent check or money orders or chain letters, report your concern to **fraud@ups.com**.

AUBURNBANK

Member FDIC | AuburnBank.com

9) **Helpful information for prevention of Fake Check Scams,** you may obtain information from www.fraud.gov (National Consumers League's Fraud Center) or **https://**www.ftc.gov. ***There is no legitimate reason why anyone would give you a check, money order, wire transfer, or direct deposit and ask you to wire money anywhere in return.***

10) To obtain a Free Credit Report:

a. To obtain a free annual credit report visit: www.annualcreditreport.com; call toll-free:877-322-8228; or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283.

Tips to Avoid Electronic Banking Scams

With ever-increasing technology, there has been a burgeoning amount of phishing and spoofing scams sent to customers. Remember, AuburnBank will not ask for your personal information through e-mail or cell phone text messages and we will never ask you to use your debit or credit number to verify your identity.

Additionally, by using AuburnBank's Internet Banking you can monitor your account every day for fraudulent activity. If you s hould ever find any fraudulent activity, please contact us immediately. For more information about how to register for AuburnBank's Internet Banking, please go to www.auburnbank.com. Additionally, by using AuburnBank's bill pay and electronic statement services, you can avoid leaving checks o r state m e n t s in your mailbox where they could be stolen and used by criminals to commit identity theft. You can get more information on these services at www.auburnbank.com. The Federal Trade Commission has more information on avoiding Identity Theft at www.ftc.gov.

Here is a list of suggestions to follow in order to avoid falling victim to scams:

1. **Be wary of any e-mail with urgent requests for personal information.** Phishers have been known to include distressing or inviting but false statements in their e-mails to get people to react right away. Recently, a number of phishers have toned down their language, as e-mail recipients have become more alert to the use of this scheme. Whichever way, the e-mail typically asks for information such as user names, passwords, credit card numbers, Social Security numbers, etc.

2. **Be cautious of e-mails that are not personalized or contain spelling errors or awkward syntax and phrasing.** Most phishing e-mails are sent in great bulk and as a result are not personalized. If you are wary of an e-mail claiming to be from AuburnBank that is not personalized, call us before responding. Many are from individuals in other countries for whom English is a foreign language, hence misspelled words and awkward syntax and phrasing.

3. **Be watchful of personalized e-mails that ask for your financial information.** Be skeptical of e-mails that contain some personal financial data, such as a bank account number and which asks for other information, for instance a PIN. AuburnBank will never ask for your personal financial information by e-mail.

4. **Do not take e-mail links to go to Web pages.** Instead, call the bank on the telephone to confirm the address, or log onto the Web site directly by typing in the Web address in your browser.

5. **Do not fill out forms in e-mail messages that ask for personal financial information.** AuburnBank will never ask you to complete such a form within an e-mail message.

6. **Only use secure Web sites or the telephone when giving out credit card numbers, account information, etc.** Verify that the Web site has a padlock or key icon at the bottom of the browser and make sure that the Internet address begins with "https" and not "http." Web sites beginning with "http" are not secure.

7. **Regularly check your online accounts and/or bank statements to make sure all transactions are legitimate**. With the click of a button, you can review your account online and check for unauthorized or unusual activity. If anything is suspicious, contact your bank and all card issuers immediately.

8. **Make sure that your browser and antivirus software is up to date and security patches applied.** To help avoid being scammed, ensure you have downloaded the latest security updates even if you are not alerted to do so.

9. **Only download apps for your mobile phone and tablet from app stores approved by the vendor.** Apps from other locations may contain malware.

10. **Signup for fraud alerts with your debit and credit card companies.** For information on how to do this with your AuburnBank debit card, go to https://www.auburnbank.com/personal.

Financial Fraud Enforcement Task Force Launches StopFraud.gov

StopFraud.gov combines resources from a wide range of federal agencies on ways consumers can protect themselves from fraud and report fraudulent activity. It also features access to the latest announcements, press releases, speeches and information regarding the Financial Fraud Enforcement Task Force.