Community Trust Bank

Protecting Yourself Against Online Threats

At Community Trust Bank, we have no higher priority than the security and privacy of your financial information. We maintain physical, electronic and procedural safeguards that comply with federal standards to protect your personal information. Community Trust Bank continually monitors and reviews all of its security protection measures. As new technology or improved practices become available we will adopt those that we believe may improve the security of your confidential financial information.

Community Trust Bank also wants to help you protect yourself against crimes targeted against consumers such as Identity Theft and E-mail "Phishing". The following information is provided to help you protect yourself from becoming a victim and some steps to take if you believe that you have been a victim of Identity Theft.

Identity Theft

What is Identity Theft?

Identity theft occurs when someone illegally obtains your personal information, such as your Social Security Number, Credit Card Number, Bank Account Number, or other identification and uses it to open accounts or initiate transactions in your name.

E-mail and Website Fraud (Phishing)

One of the most common types of e-mail fraud is sending a phony e-mail message that directs the recipient to a fraudulent website. These e-mails can look very convincing. There are some common features among many of these types of e-mail.

- **Urgent appeal**. The message may threaten some consequence if you do not respond.
- **Request for Information.** There may be a request to update or validate certain personal information.
- **Typos and errors**. Often the message is poorly written or has spelling errors within the message.

How to Prevent Being Phished

- Don't reply to any suspect or suspicious e-mail, even if it seems urgent.
- Don't click on links inside of e-mail
- Don't call telephone numbers from e-mail. Instead call the number on the company website, phone book, statement, or back of a Credit/Debit card.

How You Can Protect Yourself

- Secure your computer. Ensure that you have anti-virus and anti-spyware software and a personal firewall installed on your computer. There are many of these products available that will help you protect information on your computer or while using your computer.
- Always look for the  on websites where you are submitting any private or personal information. You can also look for the **s** in **"https"** at the beginning of the address to indicate a secure page.
- Destroy private records and statements when you are done with them. Tear, cut, shred, or burn paper items.
- Never give out checking account, credit card or Social Security numbers to any unknown caller or unsolicited contact.
- Expect your monthly financial statements and bills. If you do not get them when expected, contact the sender and ensure that they were sent and that the address is still correct.
- Review your Bank and financial statements. Verify all transactions were legitimate.
- Do not reply to, or click on, a link in an e-mail that warns you, with little notice or prior legitimate expectation, that an account of yours will be shut down unless you confirm billing or other account information. Instead, contact the company cited in the e-mail by using a telephone number or other form of communication that you are sure is genuine.
- Make a photocopy of information in your wallet. Including both sides of your drivers' license and any credit, ATM, debit or merchant cards you carry with you.
- Review your Credit Report annually. By law you can receive a free credit report each year. Look through the report carefully to see if there is any suspicious activity. If so, contact your credit card company immediately.
- This report can be requested online at **www.annualcreditreport.com**, via telephone at **877.322.8228**, and via mail at
  Annual Credit Report Request Service
  P.O. Box 105281
  Atlanta, GA 30348.5281.
  (There is a specific form for the request available on the website).

What to do if You Become a Victim of Identity Theft

If you believe that you have been the victim of identity theft. The following actions will help minimize your exposure.

Community Trust Bank customers should contact us immediately at 618.249.6218. We will secure your Community Trust Bank accounts.

- File a police report with local authorities.
- Contact the fraud departments of the 3 credit bureaus below. Place a fraud alert and request a copy of your credit report.
  1. **Trans Union: 800.680.7289**
  2. **Experian: 888.397.3742**
  3. **Equifax: 800.525.6285**

File a complaint with the Federal Trade Commission. Either at **https://www.ftccomplaintassistant.gov/** or via telephone at 877.438.4338

Additional Information

For more information on Identify Theft and other account fraud you can visit the following websites.

- National Fraud Information Center: **www.fraud.org**
- Federal Deposit Insurance Corporation: **www.fdic.gov**
- Federal Trade Commission: **https://www.ftccomplaintassistant.gov/**
- Anti-Phishing Working Group: **www.antiphishing.org**
- Microsoft: **www.microsoft.com/athome/security**