CARROLLTON BANK

Tips to Protect Your Identity

Identity theft continues to be one of the fastest growing crimes in the United States. In 2014, there were 12.7 million victims of identity fraud in the U.S., according to Javelin Strategy and Research. Frauds and scams often start with an e-mail, text message, or phone message that appears to be from a legitimate, trusted person or organization. Carrollton Bank offers these tips to keep your information – and your money – safe.

1. **Don't share your secrets.**

   Do not provide your Social Security number or account information to anyone who contacts you online or over the phone. Protect your PINs and passwords and do not share them with anyone. Use a combination of letters and numbers for your passwords and change them periodically. Avoid using easily identifiable information, such as your mother's maiden name, birthdates, the last four digits of your social security number, or phone number. Do not reveal sensitive or personal information on social networking sites.

2. **Shred sensitive papers.**

   Shred receipts, banks statements and unused credit card offers before throwing them away.

3. **Keep an eye out for missing mail.**

   Fraudsters look for monthly bank or credit card statements or other mail containing your financial information. Consider enrolling in our online banking to reduce the likelihood of paper statements being stolen. Also, don't mail bills from your own mailbox with the flag up.

4. **Use online banking to protect yourself.**

   Monitor your financial accounts regularly for fraudulent transactions. Sign up for text or email alerts from Carrollton bank for certain types of transactions, such as online purchases or transactions of more than $500.

5. **Monitor your credit report.**

   Order a free copy of your credit report every four months from one of the three credit reporting agencies at annualcreditreport.com†.

6. **Protect your computer.**

   Make sure the virus protection software on your computer is active and up to date. When conducting business online, make sure your browser's padlock or key icon is active. Also, look for an "s" after the "http" to be sure the website is secure.

7. **Protect your mobile device.**

   Use the passcode lock on your smartphone and other devices. This will make it more difficult for thieves to access your information if your device is lost or stolen. Before you donate, sell or trade your mobile device, be sure to wipe it using specialized software or using the manufacturer's recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen. Use caution when downloading apps, as they may contain malware, and avoid opening links and attachments – especially from senders you don't know.

CARROLLTON BANK

Protect Yourself Online

Though the internet has many advantages, it can also make users vulnerable to fraud, identity theft and other scams. According to Symantec, 12 adults become a victim of cybercrime every second. Carrollton Bank suggests the following to keep you safe online:

1. **Keep your computers and mobile devices up to date.**

   Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.

2. **Set strong passwords.**

   A strong password is at least eight characters in length and includes a mix of upper and lowercase letters, numbers, and special characters.

3. **Watch out for phishing scams.**

   Phishing scams use fraudulent emails and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from sources for which you are not familiar.

   a. Forward phishing emails to the Federal Trade Commission (FTC) at spam@uce.gov – and to the company, bank, or organization impersonated in the email.

4. **Be aware of Business Email Compromise and Vendor Impersonation Fraud.**

   With Business Email Compromise, legitimate business email accounts are compromised and used to send payment instructions to personnel authorized to conduct financial transactions for the business. The criminal entity will often compromise one of the businesses' officers and monitor their account for patterns, contacts and information. The criminal will often wait until the officer is away on business to use the compromised email account to send payment instructions. This makes the payment instructions more difficult to verify and, at the same time, seemingly more legitimate. The payment instructions will send money to an account controlled by the criminal.

   In instances of Vendor Impersonation Fraud, criminals impersonate a legitimate vendor or contractor and contact businesses or public-sector entities requesting to update account information. Contact can come in the form of an email, telephone call, fax, or traditional letter. In each case, the vendor account information is updated with the account number and routing information of an account owned by the fraudster. When a legitimate invoice is received, the entity processes a payment to the criminal account resulting in a loss to the entity.

   We recommend you establish sound business practices for your company to follow when processing payments or updating vendor banking information:

   - Initiate wires and ACH files using dual control — for example, file creation by one employee and file approval and release by another employee on a different computer.
   - Always confirm an email wire transfer request in person with the employee who requested the transaction.

- Authenticate requests to make a payment or change payment instructions by vendors and independently verify change in payment instructions. Use known contact information rather than confirming via contact information provided on the change request.
- Never provide password, username, authentication tools or account information when contacted. Carrollton Bank will not ask for this information. If in doubt, use a known contact list or publically available contact information to confirm the validity of the contact.
- Don't provide other non-public information. Seemingly innocent information can be used to make a fraudster believable when they contact others within the same organization.
- Transmit Wire and ACH payment/information forms only via secure means.
- Calls received from the Bank questioning the legitimacy of a payment are for your protection.

You can also visit the following websites to learn more about the Business Email Compromise scam:

FBI: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise†

FDIC: https://www.fdic.gov/consumers/consumer/news/cnsum13/wire-transfer-scams.html†

Department of Justice: https://www.ic3.gov/media/2017/170504.aspx†

5. **Keep personal information personal.**

   Hackers can use social media profiles to figure out your passwords and answer those security questions in the password reset tools. Lock down your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Be wary of requests to connect from people you do not know.

6. **Secure your internet connection.**

   Always protect your home wireless network with a password. When connecting to public Wi-Fi networks, be cautious about what information you are sending over it.

7. **Shop safely.**

   Before shopping online, make sure the website uses secure technology. When you are at the checkout screen, verify that the web address begins with https. Also, check to see if a tiny locked padlock symbol appears on the page.

8. **Read the site's privacy policies.**

   Though long and complex, privacy policies tell you how the site protects the personal information it collects. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

CARROLLTON BANK

Protect Your Mobile Device

Your mobile device provides convenient access to your e-mail, bank, and social media accounts. Unfortunately, it can potentially provide the same convenient access for criminals. Here are a few suggestions to help keep your information – and your money – safe.

1. **Use the passcode lock on your smartphone and other devices**. This will make it more difficult for thieves to access your information if your device is lost or stolen.

2. **Log out completely** when you finish a mobile banking session.

3. **Protect your phone from viruses** and malicious software, or malware, just like you do for your computer by installing mobile security software.

4. **Use caution when downloading apps**. Apps can contain malicious software, worms, and viruses. Beware of apps that ask for unnecessary "permissions."

5. **Download the updates** for your phone and mobile apps.

6. **Avoid storing sensitive information** like passwords or a social security number on your mobile device.

7. **Tell your financial institution immediately if you change your phone number** or lose your mobile device.

8. **Be aware of shoulder surfers**. The most basic form of information theft is observation. Be aware of your surroundings, especially when you're typing in sensitive information.

9. **Wipe your mobile device before you donate**, sell or trade it using specialized software or using the manufacturer's recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen.

10. **Beware of mobile phishing**. Avoid opening links and attachments in e-mails and texts, especially from senders you don't know. In addition, be wary of ads (not from your security provider) claiming that your device is infected.

11. **Watch out for public Wi-Fi**. Public connections aren't very secure, so don't perform banking transactions on a public network. If you need to access your account, try disabling the Wi-Fi and switching to your mobile network.

Report any suspected fraud to Carrollton Bank immediately. Visit IdentityTheft.com for warning signs of identity theft.

CARROLLTON BANK

Steps to Take if You Are a Victim of Identity Theft

If you suspect misuse of your personal information to commit fraud, you should take action immediately. If someone has stolen your identity, they are most likely working as fast as they can to use your information before you realize what has happened. The following are steps recommended by the Federal Trade Commission (FTC) to take if you believe your personal information has been stolen or you are a victim of identity theft. More information, including sample letters and information regarding your rights can be found at IdentityTheft.gov†.

1. **Contact your bank and credit card issuers immediately**. Customer service or fraud prevention telephone numbers can generally be found on your monthly statements or on the provider's website. Contact numbers for Carrollton Bank cards can be found here. Change logins, passwords, and PINs for your accounts.

2. **Place a fraud alert and get your credit report**. Get a free copy of your credit report at annualcreditreport.com or call 1-877-322-8228. Also, contact one of the three credit bureaus to place a fraud alert that will be reported to the other bureaus:
   - Equifax.com/CreditReportAssistance – 1-888-766-0008 †
   - Experian.com/fraudalert – 1-888-397-3742 †
   - TransUnion.com/fraud – 1-800-680-7289 †

3. **File a report with the Federal Trade Commission** either online at FTCComplaintAssistant.gov† or call 1-877-ID-THEFT (1-877-438-4338). Print and save your FTC Identity Theft Affidavit from the website.

4. **File a report with your local police department**. Take the following with you, and be sure to get a copy of your report:
   - Copy of your FTC Identity Theft Affidavit
   - Government-issued ID with a photo
   - Proof of address (mortgage statement, rental agreement, utilities bill)
   - Any proof of the theft (account statements, bills, IRS notices, etc.)

5. **Create your Identity Theft Report** by combining your FTC Identity Theft Affidavit with your police report. This will be your proof that someone has stolen your identity.

Other Steps to Take:

- **Sign up for a credit monitoring service, if offered**. While not required by law, some companies offer complimentary credit monitoring to victims of a breach, but this is not an automatic service. If you receive a notification alerting you to a data breach, read the letter carefully and take the appropriate steps to begin any free credit monitoring that may be offered.

- **Scan credit card and bank statements for other unauthorized charges**. Review all accounts (including dormant or infrequently used accounts) either online or using old statements for other charges you don't recognize. If you find unknown charges, call the financial institutions to alert them of the problem and request the account be locked or closed.

CARROLLTON BANK

- **Review your credit reports for mystery accounts**. Request copies of your credit report from annualcreditreport.com, and look for any accounts you may not recognize.

- **Maintain a written chronology of what happened**. Document the information lost and all steps you took to report the incident to the various agencies, banks, and firms impacted. Record the date, time, telephone numbers, people you talked to, any report or reference numbers and any other relevant information.

- **Implement preventive measures going forward**. Although some cases of identity theft are unavoidable, there are ways to make yourself less likely to become a victim:
  - Creating strong passwords and regularly changing them.
  - Shredding documents with personal information when disposing them.
  - Keeping personal information such as your address and phone number off social media sites, as well as any details you use for online security questions like your mother's maiden name.
  - Not carrying your Social Security card in your wallet.
  - Not clicking unknown links in e-mails.
  - Never giving personal information over the phone unless you initiated the call.
  - Never giving personal information via e-mail unless the e-mail is encrypted.

CARROLLTON BANK

Protect Your Small Business from Account Fraud

Thieves can take over your corporate accounts and make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable. Carrollton Bank offers these tips to avoid corporate account takeover and keep your small business safe.

1. **Educate your employees**.

   You and your employees are the first line of defense against corporate account takeover. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.

2. **Protect your online environment**.

   It is important to protect your cyber environment just as you would your cash and physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically.

3. **Partner with Carrollton Bank to prevent unauthorized transactions**.

   Talk to your banker about programs that safeguard you from unauthorized transactions. Positive Pay and other services that offer callbacks, device authentication, multi-person approval processes and batch limits help protect you from fraud.

4. **Pay attention to suspicious activity and react quickly**.

   Look out for unexplained account or network activity, pop ups, and suspicious e-mails. If detected, immediately contact Carrollton Bank, stop all online activity and remove any systems that may have been compromised. Keep records of what happened.

5. **Understand your responsibilities and liabilities**.

   The account agreement with Carrollton Bank will detail what commercially reasonable security measures are required in your business. It is critical that you understand and implement the security safeguards in the agreement. If you don't, you could be liable for losses resulting from a takeover. Talk to your banker if you have any questions about your responsibilities.

6. **Report any suspected fraud to Carrollton Bank immediately**.

You can also visit the following websites to learn more about how to protect your small business:

- U.S. Chamber of Commerce: Internet Security Essentials for Business†
- Federal Communications Commission: Small Biz Cyber Planner†
- Federal Communications Commission: 10 Cybersecurity Strategies for Small Business†
- Better Business Bureau: Data Security Made Simpler†
- NACHA – The Electronic Payments Association: Corporate Account Takeover Resource Center†

†Carrollton Bank makes no endorsement or claims about the accuracy or content of the information contained in these sites. The security and privacy policies on these sites may be different than Carrollton Bank.