

Fraud Assistance

Identity Theft

Identity Theft is a serious crime that is costly to the nation's economy and to all Americans, striking nearly 10 million U.S. consumers annually, and the Federal Trade Commission estimates this crime imposes \$50 billion in unnecessary costs on the nation's businesses every year.

Substantial measures are in place at Independent Bank to protect your identity and your accounts against theft and personal fraud. Stringent bank privacy policies protect your personal and financial information. Password protection for online transactions helps ensure online security. Encryption of online transactions helps protect you against hackers. We invite you to utilize the resources below:

Identity Theft Resources

- Federal Trade Commission - www.ftc.gov
- Identity Theft Resource Center - www.idtheftcenter.org
- Internet Crime Complaint Center - www.ic3.gov
- Texas Attorney General - www.texasfightsidtheft.gov
- Major Credit Bureaus:
 - Equifax (www.equifax.com) 1-888-766-0008
 - Experian (www.experian.com) 1-888-397-3742
 - TransUnion (www.transunion.com) 1-800-680-7289

When Identity Theft Happens to You

- Contact us immediately! Our customer service team will help you through the processes. Contact your credit card issuers immediately. Close your accounts, cancel your credit cards, and create new passwords for any new accounts.
- File a police report with your local police department and obtain a copy. You will need it to verify your claim with the credit reporting agencies.
- File a complaint with the Federal Trade Commission at www.ftc.gov or call toll free 1-877-438-4338.
- Check online accounts like eBay, PayPal, your email ISP (Internet Service Provider), online bank accounts, or other e-commerce accounts and everything else for which you use passwords.
- Contact the three major credit bureaus to request a "fraud alert" or security freeze be placed on your credit report. Request a free copy of your credit report to check for any suspicious activity.
- Check with the post office for any unauthorized change of address requests.
- Follow-up telephone contacts with letters and keep copies of all correspondence.

Avoid Phishing Scams

Phishing is an email scam involving fraudsters who pretend to be a legitimate business such as a financial institution, credit card company, online service provider, or retailer. Hiding behind the anonymity of the internet, they send out “official looking” emails or set up bogus websites to trick you into divulging your account numbers, passwords, social security numbers, and other sensitive data. **Independent Bank will never send email messages asking you to verify or provide personal information such as your social security number, account number, debit card number, or passwords.**

We suggest forwarding a phishing email or spoofed website to the following groups:

- reportphishing@antiphishing.org
- spam@uce.gov
- spoof@ebay.com
- File complaint with the Internet Crime Complaint Center of the FBI at www.ic3.gov.

Protect Yourself from Online Fraud

- Treat unsolicited email requests for financial information or other personal data with suspicion. Do not reply to unsolicited email or respond by clicking on a link within an unsolicited email message.
- Contact the actual business that supposedly sent the email to verify if it is genuine. Visit a website or call a phone number that you know to be legitimate.
- Prior to entering account information on any website, be sure to look for the “locked padlock” to make sure the site is secure.

Other Tips to Keep Personal Information Safe

- Review your credit reports frequently. For a free copy of your credit report go to www.annualcreditreport.com or call toll free 1-877-322-8228.
- Do not place outgoing mail in your residential mailbox.
- Implement a clean desk policy at home.
- Never give personal information over the phone or internet.
- Beware of mail, email, and telephone solicitations.
- Invest in a shredder that makes tiny pieces of confetti.
- Never leave receipts at ATMs (Automated Teller Machine), bank workstations, trash receptacles, or unattended gas pumps.
- Sign all credit cards upon receipt.
- Use a blue or black gel ink pen when signing checks and credit cards.
- Review your credit card statement as soon as it arrives.
- Check all your personal and business accounts frequently.
- Always shield your pin numbers when using an ATM.
- Only use essential information on your checks – no birth dates or social security numbers.
- Lock your bank check stock in a safe place.
- If an investment proposition seems “too good to be true” it probably is.
- Educate yourself about ID theft. Know your consumer rights.

We May Be Calling You

To protect your account, we monitor your ATM and debit card transactions for potentially fraudulent activity which may include a sudden change in locale (such as when a U.S. issued card is used unexpectedly overseas), a sudden string of costly purchases, or any pattern associated with new fraud trends around the world.

If we suspect fraudulent ATM or debit card use, we will call you in order to validate the legitimacy of your transactions. Your participation in responding to our call is critical to prevent potential risk and avoid restrictions we may place on the use of your card.

- Our automated call will ask you to verify recent transaction activity on your card.
- You will be able to respond via your touchtone keypad.
- You will also be provided a toll-free number to call should you have additional questions.

Our goal, quite simply, is to minimize your exposure to risk and the impact of any fraud. To ensure we can continue to reach you whenever potential fraud is detected, please keep us informed of your correct phone number and address at all times.

In the meantime, please be diligent in monitoring transaction activity on your account and contact us immediately if you identify any fraudulent transactions. Some additional tips on protecting yourself from debit card fraud are provided as follows:

- Unless absolutely required for a legitimate business purpose, avoid giving out your:
 - Address and ZIP code
 - Phone number
 - Date of birth
 - Social Security number
 - Card or account number
 - Card expiration date
- In stores and at ATMs, always cover your card and PIN (Personal Identification Number), and watch for:
 - Cell phone cameras, mirrors, or other tools used to view cards and PINs
 - People watching your transactions
 - Cashiers taking your card out of sight; take it to the register yourself
 - Any unusual activity at ATMs; if you feel uncomfortable, go to another ATM
- Online, you should never respond to unsolicited emails that:
 - Ask you to verify your card or account number; such emails are not sent by legitimate businesses
 - Link to websites; such sites can look legitimate but may collect data or put spyware on your computer

Your PIN is private, NEVER give it out.