Reporting Suspicious Activity

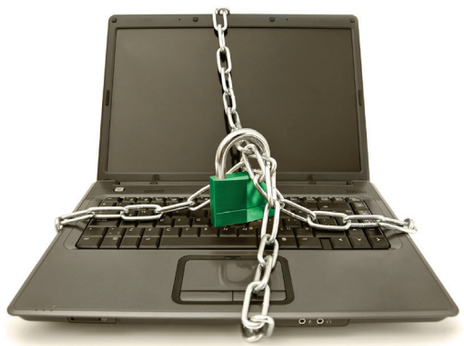
Contact Customer Service at (256) 386-5000 or (877) 865-5050 to report suspicious activity on your Bank Independent accounts or to notify us of e-mails asking you to provide Bank Independent online IDs, passwords, or other account information.

We will never ask for your personal information through an e-mail. You may also report suspicious transactions anytime using our Online Dispute Form at www.bibank.com/Online-Dispute-Form.

Helpful Tip

Take advantage of Bank Independent's Sync Complete Digital Banking Solution to greatly enhance the security of your financial information:

- eStatements and Online Banking eliminate paper trails and shredding.
- Bill Pay and Direct Deposit eliminate the risk of checks being stolen from an unprotected mailbox.
- Online Banking alerts can be set to notify you of certain transactions you might deem suspicious.



PRIVACY & SECURITY

BANK INDEPENDENT®
Radically Original™

877-865-5050 | bibank.com

Protecting your privacy, identity and financial information has never been more important to you, or to Bank Independent.

EQUAL HOUSING LENDER

Member FDIC

BANK INDEPENDENT®
Radically Original™

0315

How Bank Independent Protects You Everyday

All Bank Independent deposit accounts come with complimentary advanced protection including:

Purchase Monitoring – Your Bank Independent debit card transactions are monitored 24/7 for fraud. If purchases deviate from your normal patterns, you may be contacted to confirm purchases.

Zero Liability Protection – Under this liability program, your signature debit card purchases may be covered against fraud when you report your card lost or stolen within a reasonable period of time.

Extra ID Verification – Whether you're at a teller line or calling customer service we will ask specific questions or request identification to verify your identity.

Confidentiality Policy – Bank Independent will never share your information with a third party in an attempt to sell you other services without your permission.

Online Challenge Questions – Online and Mobile Banking now contain extra security features to ask challenge questions when accessing through a new device or location.

Transfer Authentication – We provide enhanced verification of wire and bank-to-bank transfers.

Online Fraud Notification – We provide monitoring for suspicious Online Banking and Bill Pay access.

BI Card Guardian – Enroll for an extra layer of complimentary protection from debit card fraud.

Complimentary eStatements – Protect your identity with online statements delivered to a secure inbox, not an unprotected mailbox

How You Can Protect Yourself

Prevention of identity theft and fraud begins by paying extra attention to the details, remaining aware of potential warning signs, and making it more difficult for scammers and thieves to access your information.

General Best Practices

Prevention of identity theft and fraud begins by paying extra attention to the details of your daily routines.

- **Lock up your financial documents and records** in a safe place at home
- **Limit what you carry** with you to only the identification, credit and debit cards you need. Leave your Social Security and Medicare cards at home or in a secure place
- **Be careful with your mail** and take outgoing mail to a post office collection box, promptly remove mail from your mailbox, and request a vacation hold on your mail from the post office when you'll be away
- **Consider opting out of prescreened offers of credit** and insurance by mail for five years by calling (888) 567-8688 or visiting www.optoutprescreen.com.
- **Shred sensitive documents** like receipts, credit offers, insurance forms, expired charge cards, and similar documents before putting them in your trash
- **Protect your medical information** and destroy prescription bottle labels before you throw them out
- **Exercise your curiosity** by asking your workplace, a business, your child's school or a doctor's office how your information will be handled and who will have access before you share it with them.

Identity Theft Awareness

You should always remain aware of potential signs that your information has been stolen.

For example, you may be a victim of identity theft or fraud if:

- You see unexplained withdrawals from your bank account
- Merchants refuse your checks
- You don't get your bills or other mail as expected
- Debt collectors call you about debts that aren't yours
- You find unfamiliar accounts on your credit report
- Medical providers bill you for services you didn't use
- Your health plan rejects your legitimate medical claim because records show you've reached your benefits limit
- The Internal Revenue Service (IRS) notifies you that more than one tax return was filed in your name or you have income from an employer for which you haven't worked

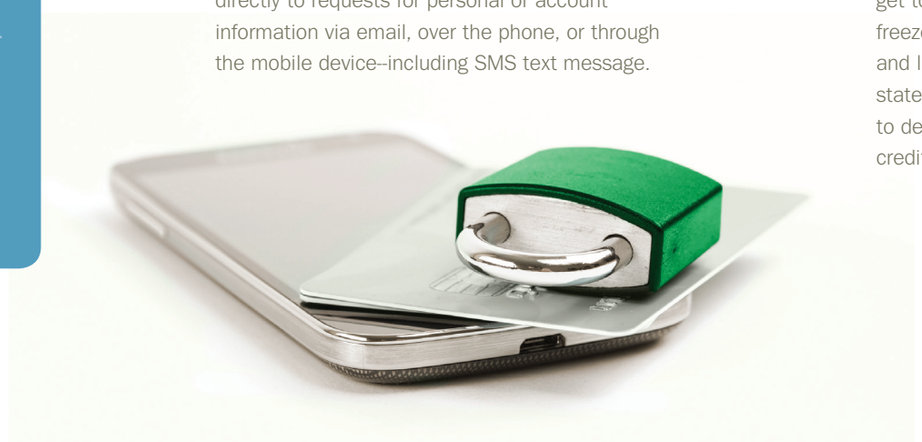
Helpful Tip

Debit cards eliminate the risk of stolen checks, but if you place a check order, request that your checks be delivered to a Bank Independent location near you, and we'll contact you when your order is available!

Online Security

The world of cyberspace presents unique challenges for protecting yourself from identity theft and fraud. There are several things you can do to make it more difficult for scammers and thieves to access your information electronically.

- **Use unique and hard-to-guess passwords** that combine letters (both upper and lower case), numbers, and symbols, and change passwords regularly. Avoid using personal information specifically, the last 4 digits of your SSN or your date of birth in your password.
- **Install security patches and software updates** as soon as they are released by verified sources
- **Sign up for security alerts** to be sent to your mobile phone or email account so that you are notified of changes to your account, personal information, or suspicious activity taking place on the account, such as unauthorized card-not-present transactions. The most common method for fraudsters to take over a victim's account is by changing the physical address.
- **Avoid using unencrypted public Wi-Fi**. SSL offers little or no protection when using unencrypted Wi-Fi hot spots.
- **Be aware of impersonators**. Never respond directly to requests for personal or account information via email, over the phone, or through the mobile device--including SMS text message.



Your Credit Report

Your credit report may show the first signs that someone has misused your information, so it's important to check your report a few times a year.

- You have the right to request a free copy of your credit report every 12 months from each of the three nationwide credit reporting companies. Visit www.annualcreditreport.com or call (877) 322-8228 to order your report(s) or learn more about how you can receive your free report.
- Credit reporting companies may charge you a fee for an additional copy of your report within a 12-month period. To buy a copy of your report, visit Equifax.com, Experian.com or Transunion.com.
- If you see errors on your credit report, like accounts you didn't open or debts you didn't incur, contact the credit reporting companies and the fraud department of each business that reported an error.
- Credit reporting companies must block identity theft-related information from appearing on a victim's credit report, but you must request this block from each of the credit bureaus.
- You may request a credit freeze on your credit file, which means potential creditors cannot get to your credit report. The length of time a freeze can stay in place and the cost to place and lift a freeze depends on state law; find your state's Attorney General's office at www.naag.org to determine applicable fees and how long the credit freeze lasts.