THE Grant COUNTY BANK
Committed To The Communities We Serve

Security Headquarters

Fraud - How to Help Protect Yourself

Fraud is a term that has become part of our everyday vocabulary. You probably hear variations of fraud ranging from identity theft, online fraud, such as phishing and pharming, to offline fraud, including credit card, phone solicitations, print fraud, check scams, and mail fraud. You can help protect your personal information and accounts by using caution when providing confidential information. Also, by keeping yourself updated on the latest fraud alerts, you can help prevent yourself from becoming a victim.

Identity Theft

Identity theft is fraud committed or attempted using the identifying information of another person without authority. Identity theft is the unlawful act of capturing, transferring, and/or using one or more pieces of another person's personal identifying information (including, but not limited to, name, address, driver's license, date of birth, Social Security number, account information, account login credentials, government passport number, employer or taxpayer identification number, or family identifiers) and using or attempting to use that information to establish or take over a credit, deposit, or other financial account ("account") in that person's name.

Identity theft falls into one of two categories:

- **True name fraud -** Establishing (or attempting to establish) an account(s) using another person's identity.
- **Account takeover -** Establishing (or attempting to establish) control of an existing account(s) without authority of the account holder. Account takeover does not include solely the posting of unauthorized transactions against an existing account, such as forged-maker signature, counterfeit, and credit card misuse.

Online Fraud

- **Phishing -** Phishers use fraudulent emails or pop-up Web pages that appear legitimate and are designed to deceive you into sharing personal or account information.
- **Pharming -** Pharming occurs when you type in a Web address and it redirects you to a fraudulent Web site without your knowledge or consent. The Web site will try to look similar to the legitimate site in hopes of capturing your confidential information.
- **Vishing -** Vishing occurs when an email is sent asking you to call a fake phone number. The number is set up to sound like a legitimate financial institution's phone system, prompting you to type in your 16 digit credit card number and expiration date to verify your information. Once you do that, however, you have just given the scammers all they need to have access to your account.

Credit Card Fraud

Credit card fraud can occur when someone takes your card and uses it without your consent. It can also happen when the card sits safely in your wallet.

Phone Solicitations

Scammers will attempt to randomly call people with hopes of luring them with cash gifts or prizes in exchange for personal account information.

Print Fraud

Scammers will use local and community newspapers to publish fake advertisements with special rates and offers. If clients call, they are asked for their personal information and for an advance payment before the transaction can be completed.

Check Scams

Scammers will overpay for an item purchased and ask the difference to be wired back. Most times the check was counterfeit or forged for a higher amount.

Mail Fraud

Mail fraud occurs when scammers illegally intercept your mail or when you receive unrealistic offers.

How to Identify Fraud

By keeping on top of your transactions, you can spot any suspicious activity. With GrantNet Online Banking you can view your transactions 24/7.

Tips on how to help identify fraud:

- Monitor your bank statements monthly.

- Review your credit report at least once year.

You are your own best protection against fraud. By staying informed, you can help protect your identity and accounts.

Phone Solicitations

Be wary of telephone scammers. If you receive a call from someone asking for personal and account information, call the company back using a phone number you know is legitimate.

Scammers use fraudulent contact information such as mailing addresses, phone and fax numbers and claim to be "third-party consultants." When unsuspecting consumers contact the scammers, the callers are asked to provide their personal and account information. Scammers then tell applicants that their loans have been approved but that they first need to make an advance payment or deposit before the loans can be advanced by wire transfer.

Check Scams

Scammers may deceive clients into responding to an illegitimate online or newspaper advertisement or may victimize clients by paying for goods with a stolen or counterfeit check for more than the agreed upon amount. The clients are then asked to return the overpayment either by a wire transfer or an official check.

Mail Fraud

Scammers may steal or tamper with your mail. Be sure to pick up the mail daily. Drop your mail in an official postal mailbox.

Help Protect Yourself from Fraud

At Grant County Bank, the protection of all your assets - including your identity - is our top priority. There are many things you can do to help secure your identity and your accounts. Here are some tips to follow.

Identity Theft:

- Don't include your Social Security Number or driver's license number on sensitive documents.
- Don't leave incoming mail lying around.
- Drop your mail in an official postal mailbox.
- Shred or destroy any junk mail before you throw it away.
- Don't respond to unsolicited requests for personal or account information.

- Use a safe deposit box to protect important documents.
- Review your credit report at least once a year.

Online Fraud:

- Look beyond the logo. To make fraudulent emails or Web sites appear real, scammers often include actual logos and images of legitimate companies. They also convey a sense of urgency, stating that if you fail to provide, update, or verify your personal or account information, access to your accounts will be suspended. It's important that you look beyond the logo and not give out your information.
- Use your spam filter. Many email services now have spam filters that minimize the amount of spam you receive. The filters can help you minimize the number of fraudulent emails in your inbox.
- Type, don't click. Even if you do open a suspicious email, don't click on any links. By clicking on the links, you could unknowingly download a virus or spyware to your computer. Even if you think the email is legitimate, type Web addresses into your browser instead of clicking on links. If the email is from an institution you do business with, use a bookmark that you have already created to visit the company's Web site.
- Change your online passwords often. The rule of thumb is to change your password every 30 to 60 days. Be creative with your passwords - stay away from obvious passwords like your ZIP code, year of birth, or sensitive information such as your mother's maiden name or your Social Security Number. Include symbols and/or upper and lower case letters so passwords cannot be easily intercepted.
- Update your anti-virus and anti-spam software. By keeping anti-virus and anti-spam software up to date on your computers, you make it more difficult for scammers to access your personal and account information. You can purchase anti-virus and anti-spyware software at major retail stores, as well as on the Internet.
- Delete emails from unknown senders with nonsensical subject lines.

Offline Fraud:

Credit Card Fraud

- Sign your cards immediately once they arrive in the mail.
- Memorize your PIN and don't write it on anything, especially something in your wallet.
- Don't enter your card online unless you're on a secure site. Don't send your credit card number in the mail.
- Keep a record of all your account numbers, expiration dates, and contact information for each issuer. This will come in handy if your wallet is lost or stolen.

- Report a lost or stolen card right away. Quick action will minimize potential loss and liability.
- Save your receipts to compare against your billing statement. When discarding receipts, tear them up or shred them.
- Monitor your statements monthly, making sure you recognize all charges. If you see any suspicious transactions, contact the bank immediately.
- Carefully review receipts for voided transactions and be sure they do not post to your account.
- Destroy your carbons. Do not leave them behind without tearing them up.
- Don't leave your purse, wallet, cards or receipts unattended. Always keep them secure or in your sight.
- Only carry cards that you need, leaving others in a safe place at home.
- Don't give out your account number unless you know and trust the company.
- In lieu of a signature on your credit card, write "verify signature on driver's license."
- Shield your hand from view of others when entering your PIN at ATMs.

Check Scams

- Use direct deposit for paychecks, Social Security payments and other regular deposits.
- Be aware of fake check scams that promise easy money for working at home, winning sweepstakes or depositing checks from foreign countries.
- Do not leave your checkbook unattended.
- Know who you are doing business with.
- Report lost or stolen checks immediately.

Mail Fraud

- Shred Documents containing your personal and financial information before placing them in the trash.
- Report an unauthorized transactions to Grant County Bank immediately.

Protecting Your Computer and Online Accounts

Protect your computers like you protect your checkbook. The following tips will help you protect your computer and your online accounts:

- Be cognizant of your surroundings when using a public computer or working on a wireless network.
- Keep your online accounts active - such as GrantNet with Bill Pay - to watch for any suspicious transactions.
- Help protect your computer and your accounts by installing anti-spyware on your computer. Anti-spyware can help prevent the collection of your personal and account information without your knowledge.

- Update your anti-virus software regularly to help protect your computer against viruses and other harmful computer codes.

How Scammers Obtain Your Email Address

Many scammers randomly generate email addresses - that's why you may have received fraudulent emails that appear to be from banks you do not have an account with. They also purchase mailing lists, obtain email addresses online from Web pages, chat rooms, online auctions, and directories or from illegitimate sources.

Grant County Bank will never trade, rent, or sell your personal information - including email addresses - to anyone. For more information on our privacy policy, visit our Privacy section on this Web site.

If You Believe You May Be a Victim of Identity Theft, You Should:

- Report the theft to each of these credit reporting agencies: Experian (888) 397-3742; Equifax (800) 525-6285; and TransUnion (800) 680-7289.
- File a police report in your local jurisdiction and retain the report number and name of the officer with whom you filed the report.
- Contact the Federal Trade Commission's Identity Theft Hotline at 877-IDTHEFT to file a complaint or go to www.ftc.gov/bcp/edu/microsites/idtheft.

Commercial Banking Customers

Safeguarding Your Information

At Grant County Bank, the security of customer information is a priority. We are strongly committed to the safety and confidentiality of your records. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. One of the best ways to avoid fraud is to become an educated user.

Small to Medium sized business and government banking accounts are being targeted by criminals every day.

Every security system in place today can and has been compromised by criminals. No system that the bank has put in place can catch 100% of fraudulent attempts.

***** Commercial Accounts and Government Accounts are not covered under Regulation E. *****

In most circumstances you will be responsible for assuming the loss on fraudulent transactions. It is vital that your following best practices:

What we expect of you:

- Establish a separate account for the origination of each type of transaction. ACH origination / Wire Transfer etc.
    - Ideally only fund those accounts with enough funds to cover the planned transactions on a daily basis. Establish dual control over the setup and creation of new user accounts on the system.
- Establish dual control over the setup of new payees on the system.
- Run summary reports of all transactions to ensure they are accurate.
- Review your transactions the next business day to determine if fraudulent activity has occurred.
- Maintain up to date anti-virus on your computer systems at all times that access financial websites.
- Patch your operating system weekly and ensure that you are updating Java and Adobe applications weekly as well. Vulnerabilities in these applications are utilized by criminals constantly.
- Ideally, dedicate a single PC for online financial transactions and prohibit any other form of web surfing on this PC.
    - Have the firewall specifically restrict access for the workstation to only the IP Addresses of the financial institutions systems. This will prevent individuals from surfing the internet on the PC.
- Utilize a unique complex password (Upper Case, Lower Case, Special Characters) at least 8 characters long.
    - DO NOT RE-USE PASSWORDS THAT YOU HAVE REGISTERED FOR AT OTHER WEBSITES!
    - Websites can be compromised and your password will be exposed.
    - Change your password every 30 days.
    - Do not utilize words in your password such as Password1.
- Never provide your account number or username / password in any written communication to the bank. This is especially true of email.
- Watch out for copycat Web sites that deliberately use a name or Web address very similar to, but not the same as the real one. The intent is to lure you into clicking through to their Web site and giving out your personal information, such as a bank account number, credit card number or GrantNet login information.
- Always use your pre-established link to access web sites. Never click on a link contained in an email.
- Utilize Security and Balance Alerts to be notified via phone, e-mail and or SMS text messages when activity occurs on the account.

What the Bank does:

- On at least an annual basis the bank examines its controls that it has implemented for online banking access.
- Based on that review the bank will determine if changes are necessary and will implement required changes on an ongoing basis.
- Reviews the current fraud trends at least quarterly to determine if changes are required in regards to current security controls and provide alerts to our customer base.
- Monitor login events 24/7 for suspicious activity on your account through a rules based online system.
- Monitor ACH transactions 24/7 at the time of transaction for suspicious activity on your account through a rules based online system.
- Monitor Wire transactions 24/7 at the time of transaction for suspicious activity on your account through a rules based online system.
- Monitor Bill Pay transactions 24/7 at the time of transaction for suspicious activity on your account through a rules based online system.
- We utilize multi-factor authentication that is in guidance of federal guidelines for online banking.
- We provide optional out of band authentication products for our commercial customers that conduct online Wire Transfer and ACH origination transactions.
- Our Customer Service Department may on occasion call to verify other information regarding your online activity should we see something of concern in your login patterns.

What the Bank does not do:

- We will never ask you for your online banking password.
- We will not contact you via email requesting you click on a link inside the email.
- All electronic communication is done through the secure email system provided within the online banking system.
- We will never send your non-public information via email unless it utilizes our security email system.

While these layered processes are designed to prevent fraud. They will not catch fraud 100% of the time. You are responsible for losses incurred on commercial and government accounts. Be vigilant and monitor your account at all times.