FRAUD BULLETIN

First Western Financial, Inc. and Affiliates ("First Western") has provided this information in an ongoing effort to maintain client awareness of Fraud and Identity Theft.

First Western will never trade, rent, or sell your personal information – including email addresses – to anyone. For more information on our privacy policy, please see related content.

Online Banking Fraud

The banking industry has seen an alarming increase in wire and ACH fraud as hackers and cyber thieves are becoming more successful in accessing bank accounts. Fraudsters are increasingly targeting small-to medium-sized businesses. Always elicit a professional IT services company to ensure your business and personal computer networking systems are secure and that virus protection is installed.

Phishing

Criminals use fraudulent emails (known as phishes) or pop-up Web pages that appear legitimate and are designed to deceive you into sharing personal or account information. The phishes often include logos of legitimate companies, content from their Web sites, and names of real employees.

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 may also obtain email addresses online from Web pages, chat rooms, online auctions, directories or other sources.

Remember, First Western will never send unsolicited emails asking you to provide, update, or verify personal or account information, such as passwords, Social Security numbers, PINs, credit or debit card numbers, or other confidential information. These requests are handled over the phone with a person from First Western.

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 and look similar to the legitimate site in hopes of capturing your confidential information.

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 is still in your possession. Your card number may have been hijacked from an online website or even captured by a skimming device at an ATM or Point of Sale terminal. Always report lost or stolen cards immediately.

Phone Solicitations

Scammers will attempt to randomly call people with hopes to lure them with cash gifts or prizes in exchange for personal or account information. A famous scam is the "Gift of $10,000 cash." The caller tells clients that they've won a gift of $10,000. Clients are asked to confirm their account and routing

numbers so that the money can be transferred to their accounts by wire. Another scam involves clients receiving a voice mail and being asked to verify possible fraudulent activities on their cards. The voice mail includes bogus phone numbers for clients to call. In regard to your cards, to be safe, always call the number on the back of your card.

Print Fraud
Scammers will use local and community newspapers publishing 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 original 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 and untrue offers.

Sweepstakes or Lotteries
Please beware of other lottery scams – especially those that originate from foreign countries. Letters notifying you that you've won a lottery or sweepstakes may require you to send money to secure your winnings. These "official" notices sometimes include fake checks. These notifications and checks are fraudulent.

To report a suspicious First Western email, Web page, or phone call, you can forward information about the email or Web page to risk@fwtb.com.

If you believe you have provided personal or account information in response to a fraudulent email, Web site, or phone call, immediately contact your First Western Relationship Manager.

At First Western Trust Bank, the protection of all your assets, including your identity is our top priority. Below you will find helpful tips to prevent you from becoming a victim of Identity Theft.

Tips on Preventing 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 receipts, junk mail or documents containing your personal and financial information 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. For more information about ordering free credit reports, go to the special Web site established by the three credit bureaus at annualcreditreport.com or call 877.322.8228.

- Look beyond the bank's 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 know, use a bookmark that you've already created to visit the company's Web site.
- Change your online passwords often. The best practice 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 numbers and letters so passwords can't be easily intercepted or guessed by others.
- 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.
- Sign the back of your Credit or Debit cards immediately once they arrive in the mail.
- Memorize your PIN and never write it on anything.
- Don't enter your credit card information online unless you're on a secure site. (Look for a lock in the bottom right hand of your screen or for "https" in the web address)
- 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 bank and credit card statements monthly, making sure you recognize all charges. If you see any suspicious transactions, contact your bank immediately.
- Don't leave your purse, wallet, cards, or receipts unattended. Always keep them secure or in your sight.
- Only carry cards that you need; leave others in a safe place at home.
- Don't give out your account number unless you know and trust the company.
- Shield your hand from view of others when entering your PIN at ATMs.
- 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.
- Report lost or stolen checks immediately to First Western by calling your local banking office or 303-531-8100.
- Notify a lender immediately if you receive a call, confirmation, or decline letter on a loan for which you did not apply.

We're committed to keeping your accounts safe from unauthorized access and your identity confidential. You are your own best protection against online fraud. By staying informed, you can help protect your identity and accounts.