INTERNET BANKING CUSTOMER AWARENESS AND EDUCATION

West Texas National Bank is committed to safeguarding your personal information. Your identity is one of the most important assets you own. It is important to keep your information safe from criminals who could potentially harm your financial well-being and reputation. The techniques used by identity thieves are becoming increasingly sophisticated; however, there are ways to keep your identity from being hijacked.

RISK CONTROL

You can protect yourself from most forms of identity theft. The best way to stay protected is to stay educated on the latest risks. Common ways identity thieves may attempt to steal your information include:

- Email scams, such as Phishing, where you receive an email from a scam artist attempting to obtain your sensitive information such as social security number, credit card information, or bank account information. You can avoid this type of scam by:
  - Not responding to an email requesting confidential information;
  - Being cautious when opening attachments, especially executable files;
  - Not clicking on any link within an email. Instead, type in the known website address for the bank or company into your web browser;
  - Not calling phone numbers within suspicious emails. Instead, call the telephone number on the company's or bank's known website.
- Internet attacks such as viruses, spyware, and keystroke loggers. Ways to protect yourself from this type of attack include:
  - Installing and maintaining up-to-date antivirus and antispyware protection;
  - Using a firewall;
  - Keeping your computer's operating system and hardware up-to-date;
  - Using only trusted websites when downloading items such as music, movies, and photographs from the Internet;
  - Being cautious when using public computers to perform any personal transaction.
- Telephone scams such as Vishing where a caller calls claiming to be from a bank or company and attempts to get information about you and/or your account. You can protect yourself from this type of scam by:
  - Verifying the identity of the caller;
  - Returning the call to a number that you confirm from another source such as a trusted website or paper statement;
  - Being suspicious anytime your personal information is requested over the phone.

Additionally, any paper statements containing your personal information should be shredded to protect from identity thieves going through your trash. Monitor your account activity regularly so that you can quickly identify any unauthorized activity. Report lost or stolen checks, debit cards, and credit cards immediately. Never keep PIN numbers with your debit and credit cards.

Information concerning mitigating identity theft risk can be found at the following locations:

United States Department of Justice
Fraud Section
http://www.justice.gov/criminal/fraud/websites/idtheft.html

Federal Trade Commission
Consumer Information – Identity Theft
http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Federal Deposit Insurance Corporation
https://www.fdic.gov/consumers/theft/

WEST TEXAS NATIONAL BANK ONLINE BANKING CONTROLS
Access to WTNB Internet Banking and WTNB BillPay requires multi-factor authentication using image and device recognition technology. Upon initial enrollment you will be required to choose a private image and pass phrase that will be presented for verification each time you access the system. If the image and pass phrase presented upon login do not match you private image and pass phrase chosen, do not enter your password, and contact the bank for further assistance.

Computers that you use frequently can be registered and a unique "cookie" will be placed on your computer for system recognition upon subsequent logins. System access from a non-registered computer will require answering challenge/response questions to verify your identity before access is granted.

Tokens are offered by WTNB as an additional layer of security when logging in to WTNB Internet Banking.

UNSOLICITED CUSTOMER CONTACT
West Texas National Bank will never contact its customers on an unsolicited basis to request their Online Banking security logon credentials such as the combination of a customer's username and password by either telephone or email. If someone claiming to be from West Texas National Bank contacts you to request this information, do not provide this information. If you receive an email that appears to be from West Texas National Bank requesting any type of personal or confidential information, do not respond to this information or click on any links in the email. Please report any activity of this nature to us at (877) 493-7862.

We may contact you to address items such as suspected fraudulent activity, any changes or disruptions in our service, or to confirm changes to your account submitted through Online Banking. If we do need to contact you, we will clearly identify ourselves and any communication will be done in a manner that protects your confidential information. **We will never ask you for your logon security credentials**. If you contact us, we will verify your identity using personal information you have provided us, but we will not ask you to provide your electronic banking credentials.

COMMERCIAL CUSTOMER RISK ASSESSMENTS AND CONTROLS EVALUATION
Commercial online banking customers should periodically perform a risk assessment and controls evaluation. This risk assessment should identify what assets or information you are

trying to protect and why; identify threats to these assets, such as potential weaknesses in storage, access, and controls; and consider the consequences of a successful attack. After performing this risk assessment, controls can be enhanced as needed to mitigate any identified risk.

AN EXPLANATION OF PROTECTIONS PROVIDED, AND NOT PROVIDED, TO ACCOUNT HOLDERS RELATIVE TO EFT UNDER REGULATON E

Regulation E, or the Electronic Fund Transfer Act, establishes the basic right, liabilities, and responsibilities of (1) consumers who use electronic fund transfer services and (2) financial institutions that offer these services. Upon opening an account used primarily for personal, family, or household purposes, you received an Electronic Fund Transfer Disclosure and Agreement that fully outlines the terms and conditions related to Electronic Fund Transfer services. Transactions that are covered under this agreement include, but are not limited to:

- Point-of-sale transfers;
- Automated teller machine (ATM) transfers;
- Direct deposits or withdrawal of funds;
- Transfers initiated by telephone; and
- Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal.

Transactions that are EXCLUDED from Regulation E include:

- Checks;
- Check guarantee or authorization;
- Wire or other similar transfer;
- Securities and commodities transfers, if the security or commodity is:
  - Regulated by the Securities and Exchange Commission (SEC) or the Commodity Futures Trading Commission (CFTC); or
  - Purchased or sold through a broker-dealer regulated by the SEC or through a futures commission merchant regulated by the CFTC; or
  - Held in book-entry form by a Federal Reserve Bank or federal agency.
- Automatic transfers by account-holding institution;
- Telephone-initiated transfers for any transfer of funds that:
  - Is initiated by a telephone communication between a consumer and a financial institution making the transfer; and
  - Does not take place under a telephone bill-payment or other written plan in which periodic or recurring transfers are contemplated.

CONTACT US

Please contact us with any questions or concerns at (877) 493-7862 and we will be happy to help. We appreciate your business!

Individuals responsible for bank information security and electronic banking activities are:

Julie Faulkner
Chief Operating Officer
(877) 493-7862 ext. 9612