First State Bank Central Texas

Electronic Funds Transfer, Internet and Mobile Banking Agreement and Disclosure for Personal Accounts

On-Line Banking Agreement (Consumers Only) Please Retain For Your Records

The Online and Mobile Banking Agreement ("Agreement") governs the use of all online and mobile banking services ("Online Services") available on a computer through a traditional internet connection at www.fsbcentex.com, on a mobile device through a mobile browser, or through our mobile application available on iOS or Android. We reserve the right to add or eliminate Online Services and the availability of Online Services may be limited by your access method or access device.

In consideration of First State Bank Central Texas (the "Bank"), issuing Login Codes, Passwords, PINS, and/or other access codes for the purpose of accessing accounts with First State Bank Central Texas, Customer agrees to the terms and conditions of the Agreement and the Electronic Funds Transfer Disclosure (the "Disclosure") herein incorporated, and any other terms and conditions as from time to time may be provided.

This agreement is revised periodically and it may include changes from earlier versions. By accessing your account and engaging in Online Services, you agree to the most recent version of this Agreement, which is always available to you online. You may withdraw your consent at any time by contacting us at 254.899.6601, or your local branch, or by email at tm@fsbcentex.com and discontinuing your use of the Online Banking Services.

NetTeller Internet Banking Services: If approved for service, Bank will provide Login Codes to be used in connection with checking accounts, savings accounts, certificates of deposit, IRAs and loan accounts with the Bank. Such Login Codes may be used to access accounts as explained below under Transfer Types and limitations in the Disclosure, to (a) transfer funds between checking and savings accounts; (b) obtain balances of checking and savings accounts; (c) obtain transaction histories on checking and savings accounts; (d) initiate a non ACH stop payment request; (e) obtain electronic statements and notices that are available (f) obtain balances and transaction histories on certificates of deposit and IRAs; (g) obtain balances and transaction histories on loan accounts.

My NetTeller: This service can be used to achieve an alternative, customizable dashboard style view of various NetTeller options. This will be an option to make as the default landing page for My NetTeller.

NetTeller OFX Direct Connect: This service will allow access to account information, pay bills, transfer money from within Quicken or QuickBooks. This system uses OFX protocol to perform these transactions.

NetTeller Virtual Wallet: This service offers a secure financial management tool within NetTeller online banking. It provides an interface to manage accounts, transactions, budget, financial goals, set alerts, and to be able to view all financial information at a glance, even accounts that are held at other banks, credit unions, credit cards, and investment accounts.

Bill Payment Service: If approved for this service, Bank will arrange to provide Login Codes that will enable the customer to initiate and authorize payments online or place a stop order on an initiated and authorized payment to third parties from a primary checking account designated for this purpose. Customer's liability, Bank's liability, and other applicable terms and conditions are set forth in the Disclosure. Except as may be indicated elsewhere, Bank does not charge for the bill payment services listed above.

Through Bill Pay you can:

- Make one time or pre-authorized automatic recurring payments to a person or business ("Payee") in the United States,
- Establish and manage electronic billing; and
- Review, change, and cancel payments.

With Bill Pay you must designate the account from which the payment will come. The Pay from Account must be either a checking or a money market account. When you issue a payment through the Bill Pay service, you authorize Bill Pay to debit your Account and remit funds on your behalf so that the funds arrive as close as possible to the scheduled payment date designated by you. You must have sufficient funds in your account to cover the amount of any Bill Payments on the scheduled payment date set for the transaction, or the transaction(s) may not be processed. NSF and/or overdraft charges may be incurred if Bill Payments exceed your account balance.

The use of Bill Pay does not alter your liability or obligations that exist between you and your billers.

Bill Pay Methods: The Bill Payment Service reserves the right to select the method in which to remit funds on your behalf to your Biller. These payment methods may include, but not limited to, an electronic payment or by check. If a check is remitted to the Biller, funds are deducted from your payment account when the check is presented to your financial institution for payment.

Bill Pay Cancellation Requests: You may cancel or edit any Scheduled Payment (including Recurring Payments) prior to the payment being processed. Once the Bill Pay Service has begun processing a payment, the payment cannot be cancelled or edited, therefore a stop payment request must be submitted.

Stop Payment Request: You may stop payment on any check that you write from your First State Bank Central Texas checking account through your Online Banking service using your personal computer, or by contacting your local branch, if the check has not already posted to your account. Your stop payment request will remain on the system for (6) months and is subject to a stop payment fee. For Bill Payments made electronically, you will need to contact the Biller directly for resolution.

FSBCentex Mobile Banking: Customers must be enrolled in First State Bank Central Texas' NetTeller Online Banking Services to use Mobile Banking Services. Bank will provide Login Codes to be used in connection with accessing checking, savings, certificates of deposit, IRAs, and loan accounts with the Bank via a mobile telephone. Such Login Codes may be used to access checking, savings, certificates of deposit, IRAs, and loan as explained below under Transfer types and limitations in the Disclosure, to: (a) transfer funds between checking and savings; (b) obtain balances of checking, savings, certificates of deposits, IRAs, and loan accounts; and (c) obtain transaction histories on checking, savings, certificates of deposits, IRAs, and loan accounts. Bank is not liable for any 3rd party fees generated from use of its Mobile Banking Service. **Standard data rates apply.**

SMS Text Message Alert Systems: Bank will provide a toll-free telephone number and/or a web site address to be used in connection with accessing checking, savings, certificates of deposits, IRAs, and loan account information with the Bank via a wireless telephone device. Such phone numbers and/or web site addresses may be used to access checking, savings, certificates of deposits, IRAs, and loans as explained below under Transfer types and limitations in the Disclosure, to: (a) obtain balances of checking, savings, certificates of deposits, IRAs, and loan accounts; (b) obtain transaction histories on

checking, savings, and loan accounts. Except as may be indicated elsewhere, Bank does not charge for the SMS text message alert services. **Standard text message rates apply.**

Security: Information you provide in connection with Online Services will be stored on secure servers and protected by advanced encryption techniques. The URL addresses are encrypted on all Internet banking transactions screens, and no sensitive information is displayed in the URL. Internet banking transactions screens have an HTML command that does not permit the screen details to be saved or viewed in cache. These commercially reasonable security measures are intended to keep your information secure and to prevent unauthorized access. **Effective security; however, is dependent on your responsible behavior in protecting your Log-in Credentials and controlling access to the devices that you use to access Online Banking Services**

Login, Codes, Identification Numbers, and Passwords: Log in Credentials means your personal ID, password, and any other unique device (such as token or fingerprint) used to access Online and Mobile Banking Services. Bank assigns Login Codes, and Identification Numbers, and Passwords. Customer agrees that electronic copies of communications are valid and agrees not to contest their validity without proof of tampering. Customer agrees that using Login Codes to access account will authenticate and validate the directions given just as customer's actual signature will authenticate and validate directions given to First State Bank Central Texas.

It is acknowledged that Login Codes and Identification Codes are confidential and that they are a security method by which First State Bank Central Texas is helping to maintain the security of customer accounts. Additionally, Bank utilizes Multi-Factor Authentication, which strengthens the safeguards in place at login by requiring additional steps to very your identity. Therefore, CUSTOMER AGREES TO PROTECT LOGIN CODES, IDENTIFICATION NUMBERS, AND/OR PASSWORDS AND NOT DIVULGE THEM TO OTHERS. CUSTOMER AGREES TO NOT USE THE "REMEMBER ME" FEATURE FOUND ON INTERNET BROWSERS TO REMEMBER LOGIN CODES, IDENTIFICATION NUMBERS, AND/OR PASSWORDS. CUSTOMER AGREES THAT IF LOGIN CODES, IDENTIFICATION NUMBERS, AND/OR PASSWORDS ARE MADE AVAILABLE BY CUSTOMER TO ANOTHER PARTY, CUSTOMER IS AUTHORIZING THE OTHER PARTY TO ACT ON BEHALF OF THE CUSTOMER FOR WHICH CUSTOMER IS RESPONSIBLE.

You should always take advantage of any security features offered by your mobile device, mobile carrier, or bank. By not using security features, it leaves your personal and financial information open to anyone that may be looking for it. Consider a screen lock on your mobile device with a password or PIN feature. Many mobile devices offer this option, as well as other customizable security settings, which can help keep your device and information secure. Do not store your PIN and personal data on your mobile devices. Depending on your mobile device, you may also have the option to use a biometric feature (such as a fingerprint scanner) on your mobile device to authenticate your identity and gain access to the Online Banking Service. If you choose to activate a biometric feature, it is your responsibility to control access to Online Banking Service just as you would with your personal ID and password. You acknowledge that any person who has a biometric feature stored in your device may be able to access your Online Banking Service. Backup your personal data, such as contacts, documents, and photos so that may be restored if your device is lost or stolen. Always accept updates and patches to your device's software as soon as it's available. These updates patch vulnerabilities and fix software issues.

Contact Treasury Management at 254.899.6601 if:

- You would like to change, disable, or revoke your password; or
- You believe that your password or other means to access Online Banking Services has been lost or stolen; or

- You believe that someone may attempt to use Online Banking Service without your consent or has transferred money without your permission.

Malware Liability: Customer assumes all risks associated with the use of First State Bank Central Texas' NetTeller Internet Banking Services, including any risk of damage to customer's personal or business computer, mobile device, software or data due to any virus, software, or any other file or code which might be transmitted or activated via Bank's NetTeller Internet Banking Services and Mobile Phone Banking Services, or customer's access to said services.

eStatements and eNotices: You have the right to receive a paper statement for any account that you access electronically and you may elect to electronically access account statements and notices ("eStatements") as detailed below. The cycle time for eStatements will be the same frequency as paper statements. Your selected documents will be delivered to the **EStatement** section of your online banking and will be presented in a format that you can view online, save to your computer, or print at your convenience. eStatements will build and retain 18 months of statements and notice history that you may access at any time. You will receive an email, to the email address on file within the Online Banking Service, when your statement is available.

Account Alerts: You may establish Event, Current Balance, Current Item and Current Personal Alerts within the Online Banking Service. All Account Alerts are sent via email or received upon log-in to the Online Banking Service. Alerts will be sent each day, at various times, when transactions occur that meet your specified criteria. You understand and agree that Account Alerts may not be sent on a "real time" basis, and may be sent at the next scheduled delivery time. Account Alerts are not intended to replace your account statement, nor are they a substitute for overdraft protection and may not prevent you from incurring overdraft fees.

Disclosure: Customer consents to receiving electronically—in lieu of written paper documents—applicable consumer disclosures, account records, and statements including the following "Electronic Fund Transfers—your Rights and Responsibilities" disclosure. **This consent will apply to all categories of electronic services that may be provided or made available electronically by First State Bank Central Texas.** This consent may be withdrawn at any time and a paper copy obtained of any electronically provided record, statement, or consumer disclosure. A fee may be charged for paper copies of records or statements. Copies of consumer disclosures will be provided free of charge. To withdraw consent or obtain a paper copy, contact First State Bank Central Texas Bookkeeping Department at 254-899-6630.

To receive electronic statements via email, customers must have the latest version of Adobe® Acrobat® Reader installed on their computer and this software is available @ www.adobe.com. Bank's NetTeller Internet Banking Service does not require any software/hardware in order to access and retain records, statements, or disclosures. The documents are in HTML format, and through an Internet browser may be printed or retained in an HTML or text file on customer's personal computer. If unable to access, retain, and print any record, statement or consumer disclosure that is provided electronically, contact First State Bank Central Texas Bookkeeping Department at 254-899-6630.

Electronic Fund Transfers (Consumers Only) – Please Retain For Your Records

This Electronic Funds Transfer Agreement and Disclosure ("Disclosure") is made to comply with federal law regulating Electronic Funds Transfer (EFT) services, and contains disclosures required by Regulation E that apply to consumer accounts. In addition, this disclosure contains information about terms and fees for some of the accounts we offer.

ACH/DIRECT DEPOSIT

Types of Preauthorized Transfers: You may arrange for us to complete the following preauthorized transfers to your deposit accounts:

- Accept direct deposits from your employer or other financial institutions to your checking or savings account.
- Preauthorized transfers to or from an account.

Fees and Charges:

- We do not charge for any preauthorized EFTs.
- We will charge $30.00 for each stop-payment order for preauthorized transfers.

FIRST STATE BANK CENTRAL TEXAS MASTERMONEY CARD/ COMBINED ATM/ POINT OF SALE (POS)/ DEBIT CARD

Types of Transactions/Transfers: You may use the card to pay for purchases from merchants who have agreed to accept the card at Point of Sale (POS) terminals within the networks identified on your card and such other terminals as the Bank may designate from time to time. Point of Sale (POS) transactions involving a refund will be credited to your Primary Account. You may also use the card to pay for purchases from merchants that accept the POS debit card with a MasterCard symbol. POS transactions in the United States can be done as signature/credit or pinned/debit. POS transactions outside of the U.S. where the card is present can only be done using your PIN. Signature transactions will NOT be allowed outside of the United States. You may use the automated teller machine (ATM) card and personal identification number (PIN) issued to you to initiate transactions at ATMs of ours, ATMs within the networks identified on your card and such other facilities as we may designate from time to time. Unless you specify a different account during Automated Teller Machine (ATM) transactions, your primary Account will be used for transactions. Your Primary Account number and information may be obtained from the Combined ATM/POS/Debit Card Request Form. At present you may use your card to (some of these services may not be available at all ATMs):

- Withdraw cash from your checking account.
- Withdraw cash from your savings account.
- Transfer funds between your checking and savings accounts.
- Obtain balance information on your deposit accounts.

Limitations on Frequency and Amount:

- You may withdraw up to a maximum of $1,015.00 (if there are sufficient funds in your account) per day at the ATM.
- You may make no more than ten transactions per day.

- You may purchase up to a maximum of $2,000.00 worth of goods and services per day, exclusive of ATM withdrawals.

Fees and Charges:

- There is no ATM withdrawal charge at machines owned by us.
- There is a Replacement Card Fee of $5.00 per card.
- International transactions will be charged a fee up to 1% of the transaction amount.

ATM Surcharges: When you use an ATM not owned by us, you may be charged a fee by the ATM operator or any network used to complete the transaction (and you may be charged a fee for a balance inquiry.)

FIRST STATE BANK CENTRAL TEXAS HOTLINE 24 HOUR TELEPHONE SERVICE: 866.424.8227

Types of Audio Response Services: You may access your deposit accounts by using a separate personal identification number (PIN) assigned to you and your account number in our audio response system. At the present time you may use the system to:

- Transfer funds between your deposit accounts.
- Give you tax information on interest earned or paid on your accounts.
- Obtain balance information on your deposit accounts.
- Determine if a particular check has cleared your account.

Limitations on Frequency and Amount:

- Transfers from savings deposit account to another account or to third parties by preauthorized, automatic, or telephonic (including data transmissions) and checks, drafts, and debit cards agreement are limited to six per month. Transfers from savings deposit account to another account or to third parties are unlimited by mail, messenger, and automatic teller machine or in person.

Fees and Charges for Audio Response Transactions:

- We do not charge for any Audio Response Transactions.

INTERNET BANKING (NetTeller)

Types of Internet Services: You may access your accounts by requesting the online banking services that uses the internet. The service is also compatible in the mobile banking environment and has the sms text message capability. We will provide you with a user identification number and password. You may reach us over the internet at www.fsbcentex.com

- Transfer from checking to savings.
- Transfer from savings to checking.
- Principal payments to Loans.
- Inquire on Checking, Savings, IRAs, CDs, and Loans.
- Online bill payment.

- Financial Institution to Financial Institution (FI to FI) transfers.
- Electronic statements and notices (eStatement and eNotice).

Limitations on Frequency and Amount:

- Transfers from savings deposit account to another account or to third parties by preauthorized, automatic, or telephonic (including data transmissions) and checks, drafts, and debit cards agreement are limited to six per month. Transfers from savings deposit account to another account or to third parties are unlimited by mail, messenger, and automatic teller machine or in person.
- Transfer from checking to savings, savings to checking amounts are dependent upon collected account balances on deposit at the time the transfer is entered.
- FI to FI transfer limitations: no more than 2 transfers per day; no greater than $5,000 in combined transfers.

Fees and Charges for Internet Transactions:

- We do not charge for any Internet Transactions.

ONLINE BILL PAYMENT

- It's Safe – Online Bill Payment uses the highest standards of encryption available.
- It's Guaranteed – Online Bill Payments are protected by the same laws that protect you from credit card fraud, limiting your liability to a maximum of $50 for any unauthorized use of your account.
- History – View your payment history for the past 180 days, adding payment convenience.

Fees and Charges for Bill Pay Transactions:

- We do not charge for any Bill Pay transactions.

The following limitations may be applicable to your accounts, except as provided by law:

Liability for Unauthorized MasterCard Point of Sale Transactions: Tell us, AT ONCE, if you believe your point of sale debit card has been lost or stolen or if there are any unauthorized transactions. Your liability for unauthorized point of sale debit card transactions that take place on the MasterCard system is Zero dollars ($0.00). Zero liability is provided under the following conditions:

- Your account is in good standing.
- You have exercised reasonable care in safeguarding your card.
- You have not reported two or more unauthorized events in the past 12 months.

We may require you to provide a written statement regarding claims of unauthorized point of sale debit card transactions. "Unauthorized Use" means that the use of your debit card by a person, other than you, who does not have actual, implied, or apparent authority for such use, and from which you receive no benefit.

These provisions limiting your MasterCard liability do not apply to MasterCard commercial cards or ATM transactions; and apply only to cards issued in the United States. With respect to unauthorized transactions, these limits may be exceeded to the extent allowed under applicable law (see Liability for Unauthorized Transfers paragraph below) only if we determine that you were grossly negligent or fraudulent in the handling of your account or point of sale debit card. The same consumer liability limits shall apply to Interlink Transaction. To notify us of lost or stolen cards, or of unauthorized transactions, call or write to us at the telephone number or address set forth below. This will help prevent unauthorized access to your account and minimize any inconvenience.

In addition to the limitations set forth above, the following limitations may be applicable to your account:

Liability for Unauthorized Transfers: Tell us AT ONCE if you believe your card, PIN, or Audio Response PIN has been lost or stolen. Telephoning is the best way of keeping your possible losses down. You could lose all the money in your account. If you tell us within two (2) business days, you could lose no more than $50.00 if someone used your card or code without your permission. If you do NOT tell us within two (2) business days after you have learned of the loss or theft of your card or code, and we can prove that we could have stopped someone from using your card or code without your permission if you had told us, you could lose as much as $500.00. Also if your statement shows transfers that you did not make, tell us at one. If you do not tell us within sixty (60) days after the statement was mailed to you, you will not get back any money lost after the sixty (60) days if we can prove that we could have stopped someone from taking the money if you had told us in time. If a good reason (such as long trip or a hospital stay) kept you from telling us, we will extend the time periods. If you believe that your card or code has been lost or stolen or that someone has transferred or may transfer money from your account without your permission, call (254) 899-6630, or write us at First State Bank Central Texas, P.O. Box 6136, Temple, Texas 76503-6136.

Business Days: For purpose of these electronic funds transfer disclosures, our business days are Monday through Friday. Holidays are not included.

Stop Payments on ATM, POS, or Debit Card Transaction: You may not place a stop payment order on any ATM, POS, or debit card transaction.

Documentation:

Periodic Statement: You will receive a monthly account statement from us for your checking account. For all other accounts you will receive a monthly account statement from us unless there are no transactions in those accounts in a particular month (in which case you will get a statement at least quarterly). You will receive a quarterly statement from us on your savings account if this is the only account you maintain and the only possible electronic transfer to or from the account is a preauthorized deposit.

Terminal Receipt: You can receive a receipt at the time you make any transfer to or from your account using one of our ATMs or a POS terminal. You may not get a receipt if the amount of the transfer is $15 or less.

Direct Deposits: If you have arranged to have direct deposits made to your account at least once every sixty (60) days from the same person or company, you can call us at (254) 899-6630 to find out whether or not the deposit has been made.

Our Liability for Failure to make Transfers: If we do not complete a transfer to or from your account on time or in the correct amount according to our agreement with you, we will be liable for your losses or damages. However, there are some exceptions. We will NOT be liable for instance:

- If through no faults of ours, you do not have any money in your account to make the transfer.
- If the money in your account is subject to legal process or other claim restricting such transfer.
- If the transfer would go over the credit limit on your overdraft line.
- If the ATM where you are making the transfer does not have enough cash.
- If the terminal or system was not working properly and you knew about the breakdown when you started the transfer.
- If circumstances beyond our control (such as fire or flood) prevent the transaction, despite reasonable precautions that we have taken.

In Case of Errors or Questions about your Electronic Transfers: Telephone us at (254) 899-6630, or write us at FIRST STATE BANK CENTRAL TEXAS, P.O. BOX 6136, TEMPLE, TEXAS 76503-6136, as soon as you can, if you think your statement or receipt is wrong or if you need more information about a transfer listed on the statement or receipt. We must hear from you no later than sixty (60) days after we sent the FIRST statement on which the problem or error appeared.

- Tell us your name and account number (if any).
- Describe the error or the transfer you are unsure about, and explain as clearly as you can why you believe it is an error or why you need more information.
- Tell us the dollar amount of the suspected error.

If you tell us orally, we may require that you send us your complaint or question in writing within ten (10) business days. We will determine whether an error occurred within ten (10) business days after we hear from you and will correct any error promptly. If we need more time, however, we may take up to forty five (45) days to investigate your complaint or question. If we decide to do this, we will credit your account within (10) business days for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within ten (10) business days, we may not credit your account.

We will tell you the results within three (3) business days after completing our investigation. If we decide that there was no error, we will send you a written explanation. You may ask for copies of the documents that we used in our investigation. If a notice of error involves an electronic fund transfer that occurred within thirty (30) days after the first deposit to the account was made, the applicable time periods for the action shall be twenty (20) business days in place of ten (10) business days. If a notice of error involves electronic fund transfer that was initiated in a foreign country, occurred within thirty (30) days after the first deposit to the account was made, or is a point of sale debit card transaction, the applicable time period for action shall be ninety (90) calendar days in place of forty five (45) calendar days. If a notice of error involves unauthorized use of your point of sale debit card with the MasterCard logo which it is used as a MasterCard point of sale debit card, we will provide provisional credit within five (5) business days after you notify us instead of within ten (10) or twenty (20) business days. We may withhold providing this accelerated provisional credit, to the extent allowed under applicable law, if the circumstances or account history warrants the delay. If we determine that previously issued provisional credit should be reversed, a Notice of Reversal of Provisional Credit will be provided to you. If we debit your account to reverse a provisional credit, we will honor checks, drafts, or similar instruments payable to third parties and preauthorized transfers from your account (without charge to you as a result of an overdraft) for five (5) business days after the notification.

Confidentiality: We will disclose information to third parties about your account or the transfer you make:

- To complete transfers as necessary.

- To verify the existence and condition of your account upon the request of a third party such as a credit bureau or merchant.
- To comply with government agency or court orders.
- If you give us your written permission.

Personal Identification Number (PIN): The ATM PIN, POS PIN or Audio Response PIN issued to you is for your security purposes. The numbers are confidential and should not be disclosed to third parties or recorded on the card. You are responsible for safekeeping your PIN(s). You agree not to disclose or otherwise make your ATM PIN, POS PIN or Audio Response PIN available to anyone not authorized to sign on your accounts.

Notices: All notices from us will be effective when we have mailed or delivered them to your last known address on our records or delivered them via Internet Banking if you have selected electronic delivery of this information using the eStatement and/or eNotice feature(s).

Enforcement: In the event either party brings a legal action to enforce this Agreement or collect amounts owing as a result of any Account transaction, the prevailing party shall be entitled to reasonable attorneys' fees and costs, including fees on any appeal, subject to any limits under applicable law.

Termination of ATM, POS and Audio Response Services: You agree that we may terminate this Agreement and your use of the ATM Card, POS or Audio Response services, if:

- You or any authorized user of your ATM PIN, POS card or PIN or Audio Response PIN breach this or any other agreement with us.
- We have reason to believe that there has been an unauthorized use of your ATM PIN, POS card or PIN or Audio Response PIN.
- We notify you or any other party to your account that we have cancelled or will cancel this Agreement. You or any other party to your account can terminate this Agreement by notifying us in writing.

Termination of service will be effective the first business day following receipt of your written notice. Termination of this Agreement will not affect the rights and responsibilities of the parties under this Agreement for transactions initiated before termination.

Preauthorized Electronic Fund Transfer:

Stop Payment Rights: If you have told us in advance to make regular electronic fund transfers out of your account(s), you can stop any of these payments. Here's how: Call us or write to us at the telephone number or address set forth above, in time for us to receive your request three (3) business days or more before the payment is scheduled to be made. If you call, we may also require you to put your request in writing and get it to us within fourteen (14) days after you call. We will charge you $30.00 for each stop payment order you give.

Notice of Varying Amounts: If these regular payments may vary in amount, the person you are going to pay will tell you, ten (10) days before each payment, when it will be made and how much it will be. You may choose instead to get this notice only when the payment would differ by more than a certain amount from the previous payment, or when the amount would fall outside certain limits that you set.

Liability for Failure to Stop Payment of Preauthorized Transfers: If you order us to stop one of the payments three (3) business days or more before the transfer is scheduled, and we do not do so, we will be liable for your losses and damages.

Other Provisions: There may be a delay between the time a deposit is made and when it will be available for withdrawal. You should review our Funds Availability Policy to determine the availability of the funds deposited at ATM's. We reserve the right to refuse any transaction which would draw upon insufficient funds, exceed a credit limit, lower an account below a required balance, or otherwise require us to increase our required reserve on the account.

Electronic Check Conversion: You may authorize a merchant or other payee to make a one-time electronic payment from your checking account using information from your check to pay for purchases or pay bills.

First State Bank Central Texas

Security Guidance for Fraud and Identity Theft Protection

First State Bank Central Texas is committed to helping you fight fraud and identity theft. Identity theft is a serious crime, occurring when your personal information is stolen without your knowledge and used to commit fraud or other crimes. Identity theft can cost you time and money, destroy your credit and ruin your good name. Skilled identity thieves use a variety of methods to steal your personal information, including:

- Dumpster diving: rummaging through trash looking for bills or other paper containing personal information,
- Skimming: using a special storage device when processing a credit/debit card to steal the number,
- Phishing: receipt of spam or pop-up messages from fictitious financial institutions in an effort to entice you to reveal personal information,
- Fraudulent Address Change: completing a fraudulent 'change of address' in an effort to divert billing statements or other information to a different location,
- 'Old Fashioned' Stealing: theft of a wallet or purse; mail, including bank and credit card statements; preapproved credit card offers; and new checks or tax information. May also involve stealing personal records from employers or bribing employees who have access.

Monitor Your Accounts: You can detect suspicious activity by regularly monitoring your financial accounts and billing statements for any charges that you did not make. Be alert to signs that require your immediate attention such as:

- Bills that do not arrive as expected,
- Receipt of unexpected credit cards or account statements,
- Notification of credit denial for no apparent reason,
- Receipt of a call or letter about a purchase you did not make.

Protect Your Personal Information

- Shred financial documents and paperwork containing personal information before discarding them,
- Protect your Social Security Number. Do not carry your Social Security Card in your wallet or purse or write your Social Security Number on a check. Give out your Social Security Number only when absolutely necessary, or ask to use another identifier,
- Never give out personal information over the telephone, through the mail or over the internet unless you know who you are dealing with,
- Never click on links sent in unsolicited emails; instead, type in a Web address you know. Use firewalls, anti-spyware and anti-virus software to protect your home computer, and keep this software current,
- Do not use obvious passwords such as your date of birth, mother's maiden name or the last four digits of your Social Security Number,
- Keep your personal information in a secure place at home, especially if you have roommates, employ outside help or are having work done in your house.

Check Your Credit: Your credit report contains information about you, including accounts you have and your bill paying history. Order a copy of your credit report each year. The Fair and Accurate Credit Transactions Act requires each of the three nationwide consumer reporting agencies to provide you with a free copy of your credit report upon request once every 12 months.

Visit www.AnnualCreditReport.com or call 877.322.8228 to order your free credit report.

You may also write to:

Annual Credit Report Service
P. O. Box 105281
Atlanta, Georgia 30348-5281

Report Fraud: Contact First State Bank Central Texas to report account fraud or if you have questions regarding fraud. You should defend against identity theft as soon as you suspect it. Place a 'fraud alert' on your credit reports that requires creditors to follow certain procedures prior to opening new accounts in your name or making changes to existing ones. The three nationwide consumer reporting agencies have toll-free numbers for placing a 'fraud alert':

Equifax: 800.525.6285

Experian: 800.397.3742

TransUnion: 800.680.7289

Placing a 'fraud alert' entitles you to free copies of your credit reports. Look for inquiries from companies you have not contacted, accounts you did not open, or debts on accounts you cannot explain. The following steps should be followed if you notice suspicious activity on your credit report:

- Close all accounts that have been tampered with or established fraudulently,
- Call the security or fraud departments of each company where an account was opened or changed without your authority. Follow up in writing, keeping copies of supporting documents,
- Use the ID Theft Affidavit at www.ftc.gov/idtheft to support your written statement,
- Ask for verification that the disputed account has been closed and fraudulent debts discharged,
- Keep copies of all documents and records of conversations about the theft,
- File a report with law enforcement officials to help you with creditors who may ask for proof of the crime,
- Report the Theft to the Federal Trade Commission. This report assists law enforcement officials across the country in their investigations.

  Online: www.ftc.gov/idtheft

  Phone: 877.438.4338 or TTY at 866.653.4261

  Mail: Identity Theft Clearinghouse
  Federal Trade Commission
  Washington, DC 20580

To learn more about identity theft and obtain additional information on responding to identity theft, please visit www.ftc.gov/idtheft or contact your local First State Bank Central Texas branch.

Online and Mobile Banking Security Awareness

Protecting Yourself from Online and Mobile Banking Fraud

The online banking industry has seen an increase in fraudulent activity. With key loggers, virus attacks and phishing scams becoming more prevalent, are you doing all you can to protect yourself from becoming a victim of fraud?

For the past several years, there has been a lot of focus on identity theft. While very serious and very damaging, there are many other ways that the "bad guys" can wreak havoc on your life and your finances. Services like the ones available from the three major credit reporting agencies and companies who provide protection against other people establishing credit or identities using your Social Security Number are very valuable and worthwhile, but true identity theft is not the only threat out there in these digital times.

Account Takeover: Many cyber criminals, also referred to as fraudsters, don't just want to steal your identity in the traditional sense or get a credit card, mortgage or checking account in your name and live their life off of your good credit history, they simply want to take your money and move on to the next victim. While most companies that do business on the Internet including Financial Institutions are very diligent in providing online protection for their customers, the first line of defense is knowledge about what you, the end-user, can do to protect yourself - an electronic way of "Looking Out for Number One." The two most prevalent types of fraud, "Keylogging" and "Phishing", occur from viruses on your computer. In both cases, the end result is the fraudster capturing your login credentials, and taking over your account.

Keystroke Logging or Keylogging: Keylogging is a method by which fraudsters record your actual keystrokes and mouse clicks. Key loggers are "Trojan" software programs that target your computer's operating system (Windows, Mac OS, etc.) and are "installed" via a virus. These can be particularly dangerous because the fraudster has captured your user ID and password, account number, Social Security Number - and anything else you have typed. If you are like most other users and have the same ID and PIN/Password for many different online accounts, you've essentially granted the fraudster access to any company with whom you conduct business. After all, they've got your login credentials so the fraudster appears to be a valid user.

Here are some ways you can prevent yourself from being a victim of keystroke logging or keylogging:

- Use Anti-Virus Software. This is the single most important thing you can do to protect your computer from viruses. There are many on the market today – some cost money while others are free. If you opt to use a free version, make sure it is being offered by a reputable company and do research on the company and its product before installing.
- Keep your Operating System up-to-date with the latest security patches.

Phishing: Phishing is a scam where Internet fraudsters request personal information from users online. These requests are most commonly in the form of an email from an organization with which you may or may not do business. In many cases, the email has been made to look exactly like a legitimate organization's email would appear complete with company logos and other convincing information. The email usually states that the company needs you to update your personal information or that your account is about to become inactive, all in an effort to get you to click the link to a site that only looks like the real thing. If you click on the link to go to the phony website and enter all of your information, you've just been the victim of a phishing attack. The fraudsters have just captured all the necessary information to access your accounts online.

No reputable business will ever email you requesting that you update your personal information, including account numbers, system passwords or Social Security Numbers via a link to their site.

Follow these guidelines to protect yourself from phishing scams:

- Never click on a link from a business requesting that you provide them with personal information.
- Pay close attention to the URL (Internet address) behind the link. Often in phishing attempts, if you hover the cursor over the link the fraudsters want you to click on, it has nothing to do with the actual company they claim to be.
- If your Financial Institution uses watermarks or personal images, do not log in unless you see the correct image on the screen.
- Report any phishing attempts to your Financial Institution.

If you are unsure that the request is valid, open a new Internet session and manually key in the business' web address. If the business genuinely needs information from you, they will have you log in to your online account to see the request. In most cases, you'll just be greeted with a message indicating that the business will never email you requesting personal information.

There is no security system available that will stop fraud if the perpetrator has all of this information, so it is imperative to take the necessary steps to prevent them from getting the information in the first place.

Online and Mobile Banking Security: Information you provide in connection with Online Services will be stored on secure servers and protected by advanced encryption techniques. The URL addresses are encrypted on all Internet banking transaction screens, and no sensitive information is displayed in the URL. Internet banking transactions screens have an HTML command that does not permit the screen details to be saved or viewed in cache. These commercially reasonable security measures are intended to keep your information secure and to prevent unauthorized access. **Effective security; however, is dependent on your responsible behavior in protecting your Log-in Credentials and controlling access to the devices that you use to access Online Banking Services.**

Protecting Your Log-In Credentials - Log in Credentials means your personal ID, password, and any other unique device (such as token or fingerprint) used to access Online and Mobile Banking Services.

- Change your passwords often. Even if your financial institution doesn't require it, it is a good practice to change your passwords at least every six months. An easy way to remember: change them when you change your clocks to adjust for Daylight Savings Time.
- Don't use the same ID and PIN/Password for every online account you have.
- Never disclose your login credentials to other people or companies.
- Do not store your ID and Password information where others could gain access to it. It is best not to write the information down at all.
- Do business with a financial institution that offers two-factor authentication for accessing your information online.
- If offered by your financial institution, take advantage of hard- or soft-tokens which provide a unique onetime-use password each time you access your account. This is especially important for business accounts with multiple users.
- If accessing information via a wireless network, ensure that the network is secure. Accessing sensitive information (or any website) over a non-secure network simply leaves the door open for criminals. Even if you aren't visiting a site where you enter an ID and password, you are still leaving your computer exposed to possible threats.

Mobile Banking Security Tips - With Mobile banking usage on the rise so are cyber security threats for mobile device users. Take measures to ensure you're do not become a victim of fraud.

- Consider a screen lock on your mobile device with a password or PIN feature. Many mobile devices offer this option, as well as other customizable security settings, which can help keep your device and information secure.

- Do not use your full or partial Social Security number as your Personal Identification Number (PIN), user ID or Password Do not store your PIN and personal data on your mobile device.

- Depending on your mobile device, you may have the option to use a biometric feature (such as a fingerprint scanner) to authenticate your identity and gain access to the Online Banking Service. If you choose to activate a biometric feature, it is your responsibility to control access to Online Banking Service just as you would with your personal ID and password. You acknowledge that any person who has a biometric feature stored in your device may be able to access your Online Banking Service.

- Always take advantage of any security features offered by your mobile device, mobile carrier, or bank. By not using security features, it leaves your personal and financial information open to anyone who may be looking for it.

- Always accept updates and patches to your device's software as soon as it's available. These updates patch vulnerabilities and fix software issues.

- Always download apps from approved sources like your mobile service provider or mobile device manufacturer's market place. Fraudulent mobile apps may capture your personal information and transmit it to their servers. Download your First State Bank Central Texas Mobile App at www.fsbcentex.com.

- Do not use free public Wi-Fi connections for your banking transactions. Use your phone carrier's internet connection for enhanced security.

- When using a mobile browser to access your account information, never click on a link of the Bank's URL, always type the URL into your browser address bar, www.fsbcentex.com to access your NetTeller Online Banking service.

- Always log out of your account when you are finished with your banking activity. No doing so leaves an opportunity where an account could be accessed prior to the inactivity auto log out feature takes effect.

- Disable Bluetooth when not in use. In public areas, others can detect your device and access it through Bluetooth. Disconnecting helps prevent others from obtaining information or sending malicious code to your device.

- Never respond to urgent email or text message claiming to be from First State Bank Central Texas or any company that request your account or personal information. This is could be "phishing" an attempt to obtain your personal information.

- Regularly delete text messages and old calendar entries, clear browser history, and delete files. Remove all information prior to disposing of, recycling or donating your device.

- Be aware of shoulder surfing while accessing mobile banking. Never leave your mobile device idle while your banking session is still active.

- Backup your personal data, such as contacts, documents, and photos so that may be restored if your device is lost or stolen. Learn how to remotely wipe your mobile device. If your device is ever lost or stolen, you should know how and be able to remotely wipe it – which means removing all of your personal data and restoring the device back to its factory state. There are apps that can also help you to locate and recover your device when lost.