FIRST STATE BANK
PRIVACY POLICY

The Board of Directors of First State Bank, Watonga, Oklahoma, acknowledges its customers' expectation that their financial and personal information is private. It is the bank's practice not to disclose customer information unless such disclosure is required by law, specifically allowed by law or requested by the customer, directly or indirectly. Further the Board recognizes the risks involved in failing to keep such information in the strictest confidence. For these reason, the directors and employees of First State Bank are expected to make every effort to fulfill the bank's duties in this area.

In order to protect the customer's privacy and to reduce the possibility of litigation, the bank's general policy, except in situations where disclosure is required or specifically allowed by law, is to require a written, signed (or otherwise authenticated) authorization from the customer regarding any request for information that is made, regardless of the source of that request (including e-mail requests) this record should be placed in the appropriate file as evidence of the proper release of the information. Exceptions may be made only if the officer or employee has received information that reasonably identifies the requester as the customer or as an authorized representative of the customer. Bank procedures will include an acceptable method of identifying the customer with reasonable certainty. If the requester cannot meet the reasonable criteria selected by the bank, the information should not be provided. The bank will use extreme care when identifying a customer or customers making electronic requests.

The Federal Right to Financial Privacy Act governs the release of information to the Federal Government, including Federal agencies and Federal courts. The Oklahoma Financial Privacy Act governs release of information to state agencies, including information sought in connection with proceedings in state courts. The requirements of these statutes will be followed.

All information related to requests for customer information shall be retained for five years. These records should be maintained in a fireproof cabinet or vault.

The Bank will give a current privacy notice to all new customers and each consumer that makes application for any bank product. If there is any change in the information that the bank may share with an affiliate or non-affiliate, the bank must mail a new notice to all existing customers before any sharing may take place.

The Board annually designates a Right to Financial Privacy Officer. This officer is responsible for coordinating all requests for financial information from state and federal agencies and in connection with court proceedings. This officer will also coordinate with other officers in order to maintain and update this policy and to provide the training needed for all bank personnel.

FINANCIAL PRIVACY PROCEDURES
FOR KEEPING INFORMATION CONFIDENTIAL

Customers must be positively identified before giving out any information. The following procedures must be followed:

- Before giving out any credit information to third parties the customer must have signed an authorization allowing the bank to do so.

- The customer must be positively identified when they call for information on their accounts. Questions to be asked include: amount and date of the last deposit, account number, Social Security number. If you are not able to positively identify the person, tell them you will call them back and give the information. The call must go to a telephone number that you can identify as the customers own or their place of work.

- Scrutinize all requests for account information or change of address. You must be able to positively identify the customer before answering requests or changing addresses.

- Report any suspicious requests for information or changes of addresses. The same person may try to get information from another employee.

- If the customer comes in the bank and is not known to you, either ask for identification or ask another employee to identify them.

- All bank employees are required to keep all information heard and seen in the bank confidential.

- Do not leave your computer signed into an information system when you leave the area.

- Put away customer information that may be on your desk, before helping the next customer.

- Shred all papers that have customer names and information on them.

- Do not be intimidated by requests for information from someone claiming to be with the government (IRS or other government agency) or a law enforcement agency. Financial institutions are not required to provide such information without a subpoena.

- Verification of checks: Get the name of the business and/or person calling to verify the check. Obtain the account number, amount, check number, the signature on the check and the names printed on the check. Check to see if the person signing is authorized and see if the check number is in sequence with the checks that have been recently paid.

- Be sure to give our privacy disclosure to each new customer and any consumer making an application for a bank product.

- Review the Privacy Policy and Procedures in the event that new products, services, marketing relationships, affiliations, or mergers are implemented. Any of these may require the bank to change their Privacy Policy and Procedures. The changes also may require a new disclosure to be developed for use and be mailed to all existing customers.

Internal review of the Privacy requirements

The Right to Financial Privacy Officer will review at least annually:

- Privacy Policy and Procedures
- Privacy disclosures
- Educate and Determine that all employees are following the rules of the policy and procedures.

RESPONSE PROGRAM FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE

In the event of unauthorized access to customers information, First State Bank will identify what types of information has been accessed or misused.

Notify FDIC as soon as the institution becomes aware of an incident involving unauthorized access.

File a SAR in situations involving Federal criminal violations.

Take steps to contain and control any incident to restrict any further access.

Notify customers when warranted.

Where an incident of unauthorized access involves customer information systems maintained by an institutions service provider it is the responsibility of the bank to notify the customers and regulator.

CUSTOMER NOTICES

The notice will include:

- An explanation of the incident and what we have done to protect the customer's information from further access.
- A recommendation that the customer reviews their account statements and immediately reports any suspicious activity.
- A recommendation that the customer periodically obtains a credit report and have any information relating to fraud deleted.
- An explanation of how the customer can obtain a credit report free of charge.
- A recommendation that the customer report any fraudulent incidents to the FTC
- Telephone numbers to use for further help.

This notice can be delivered by mail, in person or by telephone.

Your personal information and/or account information has been accessed as follows:

We have taken the following action concerning this:

We make the following recommendations:

Please remain vigilant and report any incidents of identity theft to First State Bank at (580) 623-4945.

Review your account statements and immediately report any suspicious activity to us at (580) 623-4945.

Periodically obtain credit reports and have any information relating to fraud deleted.

Beginning June 1, 2005 you can receive one free credit report each year by ordering at

www.annualcreditreport.com,

calling: 1-877-322-8228, or

writing: Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

Call the credit reporting agencies to place a fraud alert on your accounts.

Equifax	1-888-766-0008
Experian	1-888-397-3742
TransUnion	1-800-680-7289

Call the Federal Trade Commission at 877-438-4338 or submit your complaint via an online form at www.ftc.gov.

Call the Social Security Administration at 1-800-269-0271 to place a fraud alert on your name and number.

Last Updated & Approved 03/12/24