PRIVACY NOTICE

I. PURPOSE: This policy reaffirms First State Bank of Olmsted's realization of and respect for the privacy expectations and rights of our customers regarding financial information and other related information, which the Bank has or gathers in the normal course of business. It is intended to provide guidance to bank personnel as well as assurance to our customers. The Bank will also act in compliance with all applicable laws and regulations.

While the Bank is to respond to subpoenas and appropriately file suspicious activity reports, it will do so with prior consideration of applicable privacy law restrictions. Further, the Bank has a duty to report suspected criminal activity to the appropriate authorities. At the same time the Bank recognizes that its customers are entitled to a right of privacy with regard to their financial affairs.

II. STATEMENT: The Bank acknowledges the importance of the privacy, security and accuracy of customer financial information and will make every effort to protect customers' financial privacy through compliance with the federal and state laws directed at protecting customer information. The Bank will consider both paper-based customer information, as well as information obtained and maintained through electronic means.

The Bank will endeavor to provide appropriate customer notification of subpoenas, summonses, written requests for information, and oral inquiries with respect to a customer's financial information. Requests for customer information will be directed immediately to the President, who may refer the inquiries to legal counsel, as necessary.

Normally the Bank does not release customer information to any third parties, whether a government authority or other party, without receipt of an appropriate subpoena or other order, a legal requirement to do so, or the written authorization of the customer. However, the Bank reserves the right to use or release such information, at its discretion, within the confines of the legal parameters previously noted. Consideration of customer financial privacy rights will be given when filing suspicious activity reports or otherwise notifying authorities with regard to suspicious activity.

Any breach of confidentiality or variation from the Bank's Privacy Policy will be considered a serious violation of an officer or employee's terms of employment and may be grounds for termination. Officers and employees will report all breaches of confidentiality to the President for further investigation.

III. RESPONSIBILITY: The Board of Directors has the ultimate responsibility to appropriately establish and maintain this policy and assure that it is being observed in the daily operations of the Bank. The President is responsible for carrying out this policy and making recommendations to the Board of Directors as to necessary or desirable changes to the policy.

IV. PRIVACY PRINCIPLES: The Bank recognizes the following eight elements of its privacy policy, which have become standard within the banking industry:

- Recognition of customer's expectation of privacy;
- Use, collection, and retention of customer information;
- Maintenance of accurate information;
- Limiting employee access to information;
- Protection of information via established security procedures;
- Restrictions on the disclosure of consumer information;
- Maintaining customer privacy in business relationships with third parties;
- Disclosure of privacy principles to customers.

A. RECOGNITION OF CUSTOMER'S EXPECTATION OF PRIVACY: Customers of the Bank are entitled to the absolute assurance that the information concerning their financial circumstances and personal lives, which the Bank has obtained through various means, will be treated with the highest degree of confidentiality and respect. Certain expectations of privacy also contain legal rights of customers which are either granted or confirmed to them through various federal and state laws and regulations. All employees are directed by this policy to assure customers of the Bank's commitment to preserving the privacy of their information. The Bank will post a notice in all banking offices that contains an abbreviated version of this policy. That notice is included as part of this policy and is designed to be both a posted notice and a direct disclosure to customers under circumstances described later in this policy.

B. USE, COLLECTION, AND RETENTION OF CONSUMER INFORMATION: It is the policy and practice of the Bank to collect, retain, and use information about consumers and customers (both individual and corporate) only where the Bank reasonably believes the gathering of such information would be useful and allowed by law to administer the Bank's business and/or to provide products, services, or opportunities to its customers.

Before collecting information from customers, the Bank will advise customers of the intended use of their personal information, through written notice where appropriate, and will obtain the customer's consent to make releases of their information in the normal course of business and to obtain customer credit reports.

C. MAINTENANCE OF ACCURATE INFORMATION: Senior management oversees the maintenance of appropriate internal controls to address the security of customer information in both paper and electronic form. These procedures address access, storage, and disposal of confidential customer information. The Bank will make best efforts to ensure that third party service providers, under outsourcing arrangements with the Bank, protect the security and accuracy of customer information. Senior management will be kept advised of any breaches of

these procedures or any detected deficiencies, and changes in procedure will be made in an expeditious manner as needed to protect customer information. Senior management is directed to establish procedures to ensure that, to the extent practicable, all customers financial information is accurate, current, and complete in accordance with reasonable commercial standards. The Bank will respond promptly and affirmatively to any legitimate customer request to correct inaccurate information, including forwarding of corrected information to any third party that had received the inaccurate information. The Bank will further undertake to record that such corrective action was requested by the customer and follow up with any third parties to ensure that they have processed the correction.

D. LIMITATION ON EMPLOYEE ACCESS TO INFORMATION: Senior management will take all steps necessary to ensure that only employees with a legitimate business reason for knowing personally identifiable customer information shall have access to such information. To the extent practicable, access will be limited by computer access codes and granting limited access to areas in which sensitive customer information is retained. Employees will be informed at the time of their initial employment of these standards and periodically reminded of these standards during training sessions at least once during each calendar year. Willful violation of this element of this policy will result in disciplinary action against the offending individual. Inadvertent violations will be dealt with in a manner to ensure that such violations are not repeated.

E. PROTECTION OF INFORMATION VIA ESTABLISHED SECURITY PROCEDURES: The Bank will maintain appropriate security standards and procedures to prevent unauthorized access to customer information. Such procedures should prevent access by not only unauthorized employees, but others as well. Such others include but are not limited to all non-employees with otherwise legitimate reasons for being on bank premises, computer "hackers", and all intruders on bank premises.

F. RESTRICTIONS ON THE DISCLOSURE OF CUSTOMER INFORMATION: The Bank will not, except in cases allowed under the law, reveal specific information about customer accounts or other nonpublic personal information to any nonaffiliated third parties unless the customer has been provided with the required privacy notices has authorized the disclosure, and has not exercised the right to revoke such authorization (including revocation by the exercise of opt out rights after receiving notice and a reasonable opportunity to opt out of such disclosures).

G. MAINTAINING CUSTOMER PRIVACY IN BUSINESS RELATIONSHIPS WITH THIRD PARTIES: If the Bank is requested to provide personally identifiable information to a third party and that request is in all respects consistent with other elements of this policy, the Bank will accede to the request only if the third party agrees to adhere to similar privacy principles, no less stringent than set forth in this policy, that provide for keeping such information confidential.

V. DISCLOSURE OF PRIVACY PRINCIPLES TO CUSTOMERS: Disclosure of the privacy notice shall be provided to customers initially and then annually thereafter. The Bank shares nonpublic personal information as allowed by law, therefore, a simplified privacy notice will be provided to customers.

VI. SUBPOENAS: Bank customers normally will be notified by the Bank upon receipt of any subpoena or other written or oral order or request for information. However, the Bank will delay such customer notification when presented with an appropriate court order to delay notice with respect to federal subpoenas or pursuant to certain other types of federal limitations or official inquiries (a "Gag Order").

Irrespective of the Bank's commitment to customer notification regarding requests for information, the Bank will not provide notification to the customer of certain grand jury subpoenas. No one, including a customer, named in a federal grand jury subpoena will be notified of the existence of or information disclosed pursuant to a federal grand jury subpoena, in the event the subpoena is issued in connection with an investigation relating to a possible crime against any financial institution or certain regulatory agencies, or a conspiracy to commit such a crime and certain other crimes as set forth in the Bank's procedures. (This will be referred to as the "Notification Prohibition.")

VII. SAFEGUARDING CUSTOMER INFORMATION: The bank recognizes its responsibilities for ensuring that it has an effective security program in place to protect customer information and records from all unauthorized persons or forms of access. To accomplish this, the bank’s Board of Directors will approve and monitor the bank’s security program, including the following responsibilities:

- Approving a written information security program;
- Overseeing the program development, implementation, and maintenance;
- Assigning specific responsibility for program implementation; and
- Reviewing management reports.

To assess the bank's risk in regard to customer information, the bank will:

- Identify foreseeable internal and external threats that could result in unauthorized use, alteration, or destruction of customer information or information systems;
- Assess the potential damages of these threats, considering the sensitivity of the customer information; and
- Assess the sufficiency of policies, procedures, information systems, and other arrangements in place to control risks.

The bank will implement the following security procedures, as appropriate:

- Access controls on customer information, including controls to prevent pretext calling, which is when unauthorized individuals seek to obtain information by fraudulent means;
- Access restrictions at physical locations that contain customer information;
- Encryption of electronic information;
- Procedures designed to ensure that information system modifications are consistent with the bank's information security program;
- Dual control procedures, segregation of duties, and background checks for employees who have responsibilities for, or have access to, customer information;
- Monitoring procedures to detect actual and attempted attacks on information systems;
- Response programs that specify actions to be taken when the bank suspects or detects unauthorized access to information systems, including reports to regulatory and law enforcement agencies; and
- Measures to protect against the loss of customer information due to potential environmental hazards.

VIII. EMPLOYEE EDUCATION AND TRAINING: Senior management is directed to provide a copy of this policy to all bank employees and to obtain a receipt from each employee acknowledging that fact. After any amendments or modifications to this policy have been duly adopted, a copy of the amended policy will also be given to each employee, again acknowledged by receipt.

At least once during each calendar year the Bank will conduct a meeting of all employees during which matters affecting customers' rights to privacy will be discussed. Such meetings will include discussions on the following:

- The proper use of customer information;
- Procedures for maintaining security of customer information;
- The importance of confidentiality and the protection of sensitive customer information;
- Any incidents, or circumstances where security has been breached and where violations of the security of customer information has or may have been violated; and
- Any other patterns of behavior, which are covered under this policy.

Periodic audits will be conducted for compliance with the Privacy Policy, which will be reported to the Board of Directors at least annually.

IX. RECORD KEEPING AND REPORTING: The Bank will maintain a record and file of all requests for customer financial information, including a copy of the request and of the information released. The record will contain a summary of each request for customer financial information and the disposition of the request, including, at a minimum, a description of the specific information requested, the date of customer notification, whether a Gag Order or Notification Prohibition exists which prevented or delayed customer notification, the identity of the state or federal government authority requesting the information, the date of receipt of a Certificate of Compliance from a federal government authority, the date of disclosure of the information, if applicable, and any other pertinent information. The record may be made available to the customer upon request, at the discretion of bank management, unless a Gag Order has been received by the Bank or circumstances for a Notification Prohibition exist.

Neither copies of Suspicious Activity Reports nor a reference to the existence of such reports will be made available to Bank customers or any other individuals involved in the reported transactions. The Bank will retain copies of Suspicious Activity Reports and the original or business record equivalent of any supporting documentation for a period of not less than five (5) years from the date of filing. The Bank will identify and maintain supporting documentation as such, and it will be deemed to have been filed with the Bank's copy of the SAR.

Senior management will maintain a separate file for the purpose of retaining any customer complaints that relate to this policy. The information regarding any complaint should include the exact nature of the complaint, describe the corrective actions taken, and confirm that the corrective actions resolved the complaint.

Senior management will make an annual report to the Board of Directors concerning customer complaints, which shall include the frequency and nature of such complaints and corrective actions taken. Complaints of a nature sufficient to present a risk of regulatory enforcement action and/or civil monetary penalties are required to be reported if and when they occur.

Senior management will regularly test the information security program. The frequency and nature of the tests will be determined by the bank's risk assessment. These tests will be conducted by independent third parties, or staff that is independent of those who maintain the security program.

Senior management will provide the Board of Directors with an annual status report on customer information security that will include:

- Risk assessment;
- Risk management and control decisions;
- Service provider arrangements;
- Results of testing;
- Security breaches or violations and management's response; and
- Recommendations for program changes.

Additionally, periodic audits will be conducted for overall compliance with this policy, which will also be reported to the Board of Directors at least annually.

X. REVIEW OF POLICY: The Board of Directors will make a review of this policy at least once each year and make any revisions and amendments it deems appropriate. The President will be responsible for suggesting more frequent revisions as situations or changes in laws or regulations dictate.