

Financial Privacy Policy

Financial Privacy Policy

The Board of Directors acknowledges that its consumer customers' expect their financial and personal information to remain private. The Board also acknowledges the legal restrictions on the disclosure of nonpublic personal information. It is the bank's policy not to disclose such information unless disclosure is:

- Required by law,
- Specifically allowed by law or,
- Requested by the customer, directly or indirectly.

Customers with relationships established for personal, family and household use are to receive an initial written disclosure describing this policy prior to establishing a customer relationship and annually thereafter.

Officers Responsible for Compliance

The Board appointed Privacy Officer is responsible for assuring that appropriate written procedures and internal controls are adopted within each operating area of the bank to assure customer financial privacy. Responsibility for developing, implementing and complying with those procedures rests with the respective department heads and facility managers; they are responsible for information security in their areas.

Internal Controls

Each department has internal controls to assure that customer/consumer information is dispensed only as allowed or required by law or regulation. (Administrative, technical and physical safeguards for customer information are addressed in the Bank's security policy.)

The internal controls on all disclosures are to first assure that disclosures are limited to the information required and are delivered in a timely fashion. In addition, internal controls on disclosures are to assure that the facts being distributed are accurate. Whenever a customer indicates information distributed on him/her is inaccurate, the matter is to be investigated and resolved promptly. Refer to the bank's Customer Complaint Policy for any possible disclosure of customer/consumer non-personal information.

The bank will use the Model Privacy Form from Regulation P for its disclosure.

The bank maintains appropriate "Customer Identification" procedures in the areas of account documentation and monitoring of customer activity. The information gained there is used only to protect the bank from fraud and to prevent its use by others in illegal activities.

Internal controls on the filing of Suspicious Activity Reports are to incorporate:

- A committee composed of the CEO, BSA Officer, Backup BSA Officer and when needed outside counsel.
- All SAR filings are reported to the Board of Directors at its next meeting.

Independent Testing

Internal compliance audits must include a review of privacy related issues in each appropriate subject area. The review shall incorporate requirements of the law or regulation.

Training

All employees are alerted to the level of confidentiality required in banking relationships during new employee orientation and must acknowledge receipt of a copy of this policy. Training incorporates privacy-related issues in each appropriate subject area. Maintenance of the confidentiality of customer/consumer information is primary responsibility of all bank personnel. Breaches of confidentiality are addressed in the employee handbook and can serve as the basis for dismissal.

Certified 10-31-2018 LM