PRIVACY POLICY

DCI Bank

PRIVACY POLICY

DCI Bank appreciates and recognizes the trust our customers have placed in us, and we want to maintain that confidence. We recognize that our customers expect and have a right for their personal financial information to remain private and secure. Keeping financial information secure is one of our most important responsibilities. This addresses our policies and practices regarding the collection, use, retention, and security of nonpublic personal information concerning those consumers and customers of ours who obtain a financial product or service from us that is to be used primarily for personal, family, or household purposes.

NONPUBLIC PERSONAL INFORMATION

Nonpublic personal Information is nonpublic information about a customer that we may obtain when providing a financial product or service to the customer.

Sources of Nonpublic Personal Information

1. Application information. Information, such as a customer's name, address, Social Security number, assets, income and debt, which are provided to us on applications and other forms.
2. Transaction and experience information. Information about a customer's transactions and account experience, such as account balances, payment history, parties to transactions; or information about our communications with the customer, such as requests for copies of checks and our responses.
3. Consumer report information. Information from a consumer report, such as the credit-worthiness or credit history of a customer.
4. Information from outside sources. Information from outside sources regarding their employment, credit, and other relationships with the customer or verifying representations made by the customer, such as employment history, loan balances, credit card balances, and property insurance coverage.

Information We Disclose

We do not disclose nonpublic personal information about our customers or former customers to affiliates or non-affiliated third parties except as required or permitted by law.

We may disclose the customer information outlined above to companies that work for us. If personally identifiable customer information is provided to a third party, the State Bank insists that the third party adhere to similar privacy guidelines for keeping such information confidential. Examples would be companies that provide check printing or data processing.

Restricting Access

We restrict access to nonpublic personal information about our customers to those employees who need to know that information to provide products or services to the customer. Employees are authorized to access Customer Information only when they need it to provide a customer with products and services or to maintain customer accounts. Our employees are bound by a code of ethics that requires confidential treatment of customer information and are subject to disciplinary action if they fail to follow this code. Required reports on violations will also be made to regulatory and law enforcement agencies.

Safeguarding Customer Information

We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard nonpublic personal information. The bank has an affirmative duty to make certain credit information is complete and accurate.

Safeguarding customer information is an integral part of our Contingency and Emergency Preparation Policy, which includes measures to protect against destruction, loss, or damage of customer records and information due to potential environmental hazards, such as fire and water damage, or technological failure.

Our privacy policy and privacy statement is included in employee training, and new employees receive privacy training during orientation. We adhere to a “clean desk” policy, whereby files, documents, computer screens, etc. cannot be accessed by anyone without authorized access. Employee training also includes training to protect against pretext calls to gain information.

Identification and verification procedures are used when questionable/unknown persons seek a customer relationship with the bank.

DCI Bank follows the requirements and statutes of the Gramm-Leach-Bliley Act (GLB Act), the Fair Credit Reporting Act (FCRA), the Right to Financial Privacy Act (RFPA), and the Bank Security Act (BSA)

Distributing Privacy Notice

An initial privacy notice is given to each new customer at the time a new customer relationship is established, either in his/her new account packet or new consumer loan information. A privacy notice is given to an existing customer when the bank provides a new financial product or service.

Copies of our customer notice are mailed annually to all customers who have deposit, loan, box holder or escrow accounts.

POLICY REVIEW

These policies and procedures shall be reviewed by the bank’s Board of Directors at least annually.

Approved by Board of Directors January 22, 2024.