Privacy & Security

Privacy Policy

What does First State Bank do with your personal information?

Why?
Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

What?
The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and income
- Account balances and payment history
- Credit history checking account information

When you are *no longer* our customer, we continue to share your information as described in this notice.

How?
All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons First State Bank chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does First State Bank share?	Can you limit this sharing?
For our everyday business purposes - such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes - to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes - information about your transactions and experiences	No	We don't share
For our affiliates' everyday business purposes - information about your creditworthiness	No	We don't share

For our affiliates to market to you	No	We don't share
For non-affiliates to market to you	No	We don't share

What we do.
How does First State Bank protect my personal information?
To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.

How does First State Bank collect my personal information?
We collect your personal information, for example, when you

- open an account or deposit money
- make deposits or withdrawals from your account or apply for a loan
- use your debit card

We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.

Why can't I limit all sharing?
Federal law gives you the right to limit only

- sharing for affiliates' everyday business purposes—information about your creditworthiness
- affiliates from using your information to market to you
- sharing for non-affiliates to market to you

State laws and individual companies may give you additional rights to limit sharing.

Definitions
Affiliates - Companies related by common ownership or control. They can be financial and non-financial companies.
**First State Bank does not share with our affiliates*

Non-affiliates - Companies not related by common ownership or control. They can be financial and non-financial companies.
**First State Bank does not share with non-affiliates so they can market to you.*

Joint marketing - A formal agreement between non-affiliated financial companies that together market financial products or services to you.
**First State Bank does not jointly market*

Security Policy

First State Bank values the trust our customers place in us and the Bank is committed to ensuring the security and confidentiality of customer information and protecting that information. Information about our customers is held in confidence by the Bank and no employee of Bank shall divulge any non-public information of a customer or discuss the business of a customer with anyone outside the bank without the customer's prior written consent or as permitted by law.

It is the policy of Bank to comply with all requirements imposed on the Bank by the Gramm-Leach-Bliley Act of 1999 regarding the safekeeping of customer information. The Bank follows its established standards for administrative, technical and physical safeguards of customer records. Additionally, the program shall meet the standards mandated by the interagency guidelines establishing standards for safeguarding customer information.

The Bank will collect, retain, and use the information about customers only where such information is believed to be useful and allowed by law to administer the business of Bank to provide products, services and other financial opportunities to its customers.

The Bank will review the measures that it has taken to safeguard customer information. The review takes into account the on-going changes in technology and the internal and external changes that the Bank goes through in addition to the complexity and scope of the Bank's activities. Not only is the focus on compliance with this part of the GLBA but also on

the legal ramifications that arise from noncompliance.

Information Security Officer

The Board of Directors of Bank shall designate a senior officer of the Bank as its Information Security Officer and annually approve the information security program. The Information Security Officer shall report to the Board at least once a year and more frequently, if deemed necessary either by the Board or the Information Security Officer.

The Information Security Officer shall design, review and inform the Board of the security program as to its ability to protect against anticipated threats to the integrity of such information and against unauthorized access or use of such information to ensure the information remains secured and confidential. The Information Security Officer shall monitor, evaluate and suggest adjustments to the Board as appropriate as needed but not less than once a year.

Douglas J. Sheppard has been appointed as the Information Security Officer by the Board of Directors to maintain compliance with all aspects of the Customer Information Security Policy.

Identifying Risks

Management shall identify the reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems.

Passwords/Authorized Users

Access to customer information is limited only to authorized individuals and the Bank maintains appropriate security standards and procedures to restrict access.

All employees of the Bank that require access to the Bank's computers to perform their duties shall be given a unique password and user identification code for use in logging onto the Bank's system. The Information Security Officer will review user access/profile listings on a regular basis. Passwords shall be designed to not be easily decipherable. All passwords shall be modeled to the tasks that the employee holding the password requires access to perform their duties and no others. All passwords shall be changed as needed, but not less than once every 90 days. Password length, timeout intervals, hours of access and lockouts will be utilized to further limit access.

Whenever a password holder's employment with the Bank is terminated, that employee's password is to be invalidated. Dual control procedures and segregation of duties are utilized for employees with access to customer information and the Bank takes any necessary disciplinary measures to enforce employee privacy responsibilities.

Physical Security

The Bank's facility and equipment shall be physically secure from damage and secure from unauthorized access. The Bank's personal computers shall be kept in secure areas and removable disks with Bank data shall be kept in secured areas when not in use. Software is held in the Bank vault under limited access and all of our irreplaceable records are kept in the vault or in fireproof safes and filing cabinets.

All information on the Bank server is backed up at the Bank. In addition to magnetic cartridge and tape files, references and printed documentation are stored off-site at Fiserv (our data processor). File backups are executed daily at Fiserv and the Bank's server is backed up daily. Fiserv stores backup media in a secure storage facility in Des Moines and the server backups are stored in the Bank vault.

Network security and operating systems are maintained on a regular basis through patches, updates, etc. In addition, virus protection is maintained on all systems. These security systems are routinely tested by an independent third party.

In the event of a natural disaster or other cause that disrupts the Bank's operations, the Bank has a recovery plan that will enable it to resume operations as quickly as possible. In addition, Fiserv maintains, and at least annually, tests a disaster recovery program for their site.

The Bank's hardware, software, computer-generated data, custom software, the LAN, and all other aspects of the Bank's computer system are an integral part of the Bank's disaster recovery policy, which is addressed in a separate policy statement.

Personal Computers

Important information is stored by personal computers in the Bank and can be changed or deleted by anyone using

them; therefore, the PCs in the Bank must be subject to controls.

No employee shall bring any personally owned personal computer, any personal computer disk, or any software onto Bank premises, or install any such item on a Bank PC, without prior approval of the Information Security Officer. In addition, no personal computer owned or leased by the Bank shall be moved from its location without permission of the Information Security Officer.

All third party developed software installed on any Bank PC shall be appropriately licensed from the software's vendor as the Bank will permit no unauthorized copies of copyrighted software to be used in the Bank's personal computers.

No one shall use any Bank PC to access the Internet or any similar service for any purpose except the Bank's business needs.

E-Mail

Customers may communicate with employees of the Bank through the use of e-mail and employees may communicate with one another through the use of e-mail.

The Bank's e-mail system may be used only for Bank related business and for no other purpose. Employees of the Bank shall not use the Bank's e-mail system for any purpose other than the communication of Bank business. Customers of the Bank shall be discouraged from using the Bank's e-mail system to communicate with an employee for any purpose other than the Bank's business.

Any communication from a customer received through the Bank's recommendations based on findings or corrective actions are followed. Summary reports will be presented to the Board at least annually.

Questions

Call 641-435-4943 or go to www.fsb-nashua.com