



Privacy Policy

TABLE OF CONTENTS

PURPOSE	1
RESPONSIBILITIES	1
INFORMATION THE BANK COLLECTS.....	1
INFORMATION THE BANK MAY SHARE	2
WHY WE SHARE INFORMATION	2
Limiting Sharing.....	2
THIRD PARTIES	2
SECURITY PROCEDURES	3
ENFORCEMENT	4
POLICY ADMINISTRATION.....	4
EXEMPTION PROCESS	4
FURTHER GUIDANCE	4
ADDITIONAL REFERENCES.....	4

South Shore Bank		
Responsible Dept(s):	Date last revision	February 2021
Risk and Compliance / Marketing	BOD Approval Date	February 2021

PURPOSE

South Shore Bank and its subsidiaries, trustees, directors, officers, and employees (hereafter referred to as “SSB” or “the Bank”) recognize the obligation maintain to the privacy and confidentiality of our clients’ non-public personal information (“PI”), as well as the nature of relationships between clients and the Bank. It is the Bank’s policy to comply with all federal and state laws and regulations relating to the privacy of our clients, consumers, and employees.

To help clients better understand how the Bank protects PI, a Privacy Notice is distributed to clients that describes its policies and practices. The Privacy Notice will be mailed annually should the Notice change and is also available on the Bank’s website.

Except as permitted by law or as otherwise described below, the Bank does not disclose any PI about its current, or former clients to anyone. The Bank may use PI that it collects and maintains to support products and services it provides. The Bank does not sell lists, client names or account information.

RESPONSIBILITIES

Board of Directors - The Policy will be approved by the Board of Directors and reviewed by the Board of Directors on an annual basis unless the Board specifies otherwise.

Risk and Compliance Department – Responsible for establishing and maintaining the Bank’s Privacy Program, including development and maintenance of this policy.

Marketing Department – responsible for communicating the Bank’s updated privacy notice to customers.

South Shore Bank Employees – All Bank employees and third parties are expected to comply with this policy.

INFORMATION THE BANK COLLECTS

The Bank collects, retains, and uses PI about clients from various sources including the following:

- Information the Bank receives on applications or other forms, including, but not limited to, identifying information such as address, telephone number, e-mail address, social security number, date of birth, mother’s maiden name, assets, income and other debts;
- Information about transactions and relationships with the Bank or others, such as account balance, payment history, overdraft history, parties to transactions or information about communications with the client; and

- Information the Bank receives from a consumer-reporting agency, such as a credit history.

INFORMATION THE BANK MAY SHARE

The Bank is permitted under law to disclose PI about clients to other third parties in certain circumstances. For example, the Bank may disclose PI to its data processing servicer to process account transactions and with others for loan originations, such as attorneys, appraisers, and title insurance companies. In addition, the Bank must respond to government subpoenas and report to credit bureaus. The Bank does not use, retain, or disclose any personal medical information about clients for marketing purposes or to make credit decisions.

WHY WE SHARE INFORMATION

The Bank uses information that it collects to better serve clients in the areas of fraud prevention, more efficient service of accounts, improved processing of transactions, verification of available funds, validation of creditworthiness and compliance with laws and regulations. Employees may access information when needed to maintain accounts or to provide services.

Limiting Sharing

Information regarding how a client may restrict the sharing of PI is set forth in the Privacy Notice.

THIRD PARTIES

Customer non-public personal information shall not be disclosed to third parties without first providing a privacy notice compliant with Regulation P, 12 CFR 1016, subject to the exceptions provided in Regulation P, sections 1016.13, 1016.14, and 1016.15, summarized below:

Section 13 permits the institution to provide consumer information to a nonaffiliated third party to perform services for the institution or functions on the institution's behalf if the institution has provided the privacy notice to the consumer and the institution has entered into a contract with the third party. The contract must require the third party to maintain the confidentiality of the information to at least the same extent that the institution must maintain its confidentiality. The contract also must limit the third party's use of the information solely to the purposes for which the information is disclosed or for permitted purposes under Section 14 or Section 15.

Section 14 permits the institution to provide information about a consumer to nonaffiliated third parties without providing the affected consumer either the privacy notice or the opt out notice when the information is provided to service or process a financial product or service requested or authorized by the consumer. It also allows providing information to nonaffiliated third parties as necessary to carry out a transaction for a consumer or to administer or maintain the product or service of which the transaction is a part.

Section 15 provides additional exceptions under which the institution may disclose consumer information to nonaffiliated third parties and nonaffiliated third parties to whom consumer information may be disclosed that do not have to be described in the institution's privacy notice and from which the consumer may not opt out. The list includes:

- Information disclosures made with the consent of or at the direction of the consumer, provided that the consumer has not revoked the direction or consent.
- Information disclosures to protect the security of the financial institution or the confidentiality of its records, or to protect against actual or potential fraud or unauthorized transactions, to control risk or to resolve consumer disputes or inquiries.
- Information disclosures to persons holding a legal or beneficial interest relating to the consumer or persons acting in a fiduciary or representative capacity relative to the consumer.
- Information disclosures to the financial institution's attorneys, accountants, auditors, agencies rating the financial institution or agencies assessing the financial institution's compliance with industry standards.
- Information disclosures specifically permitted or required by law (and in compliance with the Right to Financial Privacy Act) to the federal government.
- Information provided to a consumer reporting agency in accordance with the Fair Credit Reporting Act.
- Information disclosed to a nonaffiliated third party in connection with the proposed or actual sale, merger, transfer or exchange of a financial institution or an operating unit of a financial institution.
- Information disclosed to comply with a properly authorized subpoena or summons, or to regulatory authorities having jurisdiction over the financial institution.

The Bank may exchange limited PI with companies that conduct marketing services on its behalf or with other financial institution partners to offer jointly endorsed financial products or services.

The Bank does not have any control over the disclosure or use of *public* personal information. Other third parties may use the information to contact clients about their products, without any involvement by the Bank.

SECURITY PROCEDURES

The Bank also takes steps to safeguard client information. The Bank restricts access to personal and account information to those employees who need to know that information to provide products or services. Employees will be provided with training for privacy rules and regulations at time of hire and ongoing annually. For purposes of compliance with Section 314(b) of the U.S.A. Patriot Act, no employee other than the institution's Information Security Officer shall divulge financial information or records of a customer to anyone outside the institution. It is also Bank policy to cooperate with governmental agencies in their properly made, legitimate requests for information. Employees who violate these standards are subject to disciplinary measures. The Bank maintains physical, electronic, and procedural safeguards that are designed to comply with federal standards to guard PI.

ENFORCEMENT

The Bank reserves the right to take appropriate disciplinary action to ensure compliance with policies, standards, and procedures. Any employee found to have violated this policy will be reported to his/her supervisor and to Human Resources Department and may be subject to disciplinary action, up to and including termination of employment.

POLICY ADMINISTRATION

The Policy will be approved by the Board of Directors and reviewed by the Board of Directors on an annual basis unless the Board specifies otherwise.

The Risk and Compliance and Marketing Departments are responsible for developing and maintaining the policy.

Business areas are expected to comply with this policy upon publication. Inability to comply with a new policy or standard or a modified existing policy or standard requires a written request for exemption. If, at any time, a business area cannot comply with an established policy or standard, a request for exemption must be submitted to the Risk and Compliance, and Marketing Departments immediately.

EXEMPTION PROCESS

An exemption from policy and/or standards is necessary when a particular control or responsibility cannot be adhered to. The exemption process is intended to ensure that all reasonable alternatives are evaluated, and that compensating controls are adequate to reduce risks to an acceptable level.

FURTHER GUIDANCE

Any specific questions about this policy should be addressed to the Directors of Risk and Compliance, and Marketing.

ADDITIONAL REFERENCES

The Risk and Compliance, and Marketing Departments maintain this and other related publications. Other topics that relate to this policy can be found in those Departments.