Date Last Approved: May 17, 2023

CONSUMER PRIVACY AND INFORMATION SECURITY POLICY

Regulation P - Gramm-Leach-Bliley Act

The financial services industry is rapidly changing and being shaped by technology, which is literally changing the way Primary Bank (the "Bank") conducts its business. To be successful in this environment, the Bank must continue to grow and ensure that our customers are confident that their financial affairs will be expertly and confidentially managed.

Bank customers have access to a broad range of products and services such as basic banking products, loans, and online banking. To deliver these products and services effectively and conveniently, it is extremely important that the Bank uses technology to manage and maintain certain customer information while ensuring that customer information is kept confidential and protected.

The safeguarding of customer information is an issue that the Board of Directors (the "Board") of the Bank takes seriously. The Board maintains its continuing commitment to the proper use and protection of customer information and has established and affirmed the following Principles of Privacy as the Consumer Privacy and Information Security Policy (the "Policy") of the Bank. This Policy and the accompanying Principles follow the Gramm-Leach-Bliley Act (the "Act") and Regulation P, Privacy of Consumer Financial Information (12 CFR Chapter III, Part 332). This Policy will be used to guide the Bank in serving the privacy needs of its customers and protecting confidential information.

Customer's Expectation of Privacy: The Bank believes the confidentiality and protection of customer information is one of its fundamental responsibilities. While information is critical to providing quality service, it is recognized and understood that one of the Bank's most important assets is the trust of its customers. The safekeeping of customer information is a priority for the Bank.

Collection, Use and Retention of Customer Information: The Bank limits the use, collection, and retention of customer information to what it believes is necessary or useful to conduct its business, provide quality service, and offer products, services, and other opportunities that may be of interest to customers.

The Bank will carefully handle information it obtains about a visitor to its web site. The Bank believes that the confidentiality and protection of its web site visitor information is another of its fundamental responsibilities. Anytime someone visits the site, the following information is collected and stored:

1. The name of the domain from which they access the Internet, the date and time.
2. The Internet address of the website they left to visit us.
3. The names of the pages they visit while at our site; and
4. The Internet address of the website they then visit.

To do this, the Bank's web server will write a "cookie" to the individual's hard drive upon their first visit to the site. This electronic file is tracked during the visit and helps the Bank understand which parts of its site visitors find most useful and where they are likely to return over time. This information allows the Bank to improve the site and make it more useful.

If a consumer submits an online application or sends an e-mail:

1. The Bank may enter the information into its electronic database.
2. Consumers may also be contacted for additional information.
3. Most of the forms on the Bank's website use encryption to send information across the Internet. This is the case where confidential information, such as account numbers or social security numbers, is requested.
4. The Bank has requested that consumers do not send confidential information via e-mail. E-mail is not necessarily secure against interception. If the communication is extremely sensitive, or includes personal information such as account numbers, credit card numbers, or social security numbers, we have instructed the consumer to call us, use a secure/encrypted e-mail system, or send the information by regular mail instead.
5. The Bank will not obtain personally identifying information about any consumer when they visit our site unless they choose to provide such information to us.

Maintenance of Accurate Information: The Bank recognizes that accurate customer records must be maintained. To accomplish this, the Bank has established procedures to maintain the accuracy of customer information and to keep such information current and complete. These procedures include responding to requests to correct inaccurate information in a timely manner.

Limiting Employee Access to Information: Bank employees' access to personally identifiable customer information is limited to those with a business reason to know such information. Employees are educated on the importance of maintaining the confidentiality of customer information and on this Policy. All Bank employees are responsible for maintaining the confidentiality of customer information and employees who violate this Policy and Principles are subject to disciplinary measures.

Protection of Information via Established Security Procedures: The Bank recognizes that a fundamental element of maintaining effective customer privacy is to provide reasonable protection against unauthorized access to customer information. Therefore, the Bank has established appropriate security standards and procedures to guard access to customer information.

Restrictions on the Disclosure of Customer Information: When sharing customer information with unaffiliated companies, the Bank places strict limits on both the specific information shared and on who receives information about customer accounts or other personally identifiable data. Information is specifically identified as "Public Personal Information" and "Non-Public Personal information." The Bank may share Public information with such companies if they provide a product or service that may benefit customers. In sharing public information, the Bank carefully reviews the company and the product or service to ensure that it provides value to customers. The Bank shares the minimum amount of information necessary for that company to offer its product or service.

The Bank will not share Non-Public Personal Information except as permitted by law while its business (for example, with consumer reporting agencies and government agencies; when legally required or permitted in connection with fraud investigations and litigation; in connection with acquisitions and sales; in the audit process or the secondary market sale of loans; and at the request or with the permission of a customer).

Maintaining Customer Privacy in Business Relationships with Third Parties:

If the Bank provides personally identifiable customer information to a third-party with which the Bank has a business relationship, it will insist that the third-party keep such information confidential, consistent with the law and the conduct of the business relationship.

Disclosure of Privacy Policy to Customers: The Bank recognizes and respects the privacy expectations of its customers and wants customers to understand its commitment to privacy in the use of customer information. Because of its commitment, the Bank has developed its Policy and these Privacy Principles which are made readily available to customers. The list of Privacy and Web Site Principles has been posted on the Bank's Web Site. The Bank has also prepared a consumer privacy disclosure titled "WHAT DOES PRIMARY BANK DO WITH YOUR PERSONAL INFORMATION" which is provided to every consumer customer when they open an account with the Bank and anytime thereafter when material changes are made to the privacy disclosure.

Customers who have questions regarding the privacy of their information will be directed to contact the Bank at 1-603-310-7200 or to email the Bank at webmaster@primarybanknh.com.

This Policy and these Principles apply to individuals, and the Bank reserves the right to change these Privacy Principles, and any of the policies described above, at any time without prior notice. In accordance with the requirements of the Act, changes to this Policy which allows for sharing of Non-Public Personal Information with non-affiliated third parties not identified in this Policy will require re-disclosure to the consumer which clearly outlines those changes, and an option will be provided for the consumer to decline – or "opt out" – of the sharing of any Non-Public Personal Information.

This Policy provides for general guidance and does not constitute a contract or create legal rights and does not modify or amend any agreements the Bank has with its customers.

Information Security Objectives: Customer information is an asset and must be protected against accidental or intentional misuse. Customer information must be kept secured and confidential, and safeguarded against unauthorized access by non-Bank personnel, and must not be sold, exchanged, or given away without prior written consent of the customer.

Working with Independent Service Providers:

As the Bank periodically works with independent service providers, it must ensure that providers have security programs that meet the security objectives of this Policy.

Threats to Security Controls: The Bank must take all measures possible to identify immediate or potential threats to the Bank's security controls, including:

- Proper disposal of confidential information
- Securing of confidential information
- Computer access to confidential data
- Employee violations of the Policy
- Computer hackers
- Ransomware attacks
- Unauthorized transaction to customer accounts
- Password integrity

Any breaches or attempted breaches of security must be reviewed and reported to the appropriate legal authorities, Senior Management, and the Board.

Other Important Information:

For California Residents, only: "How Primary Bank responds to your browser's 'Do-Not-Track' signal."

Primary Bank does not respond to your 'Do-Not-Track' signal settings, nor do any of our third-party web site operators respond to 'Do-Not-Track' settings in consumers' browsers.

Neither Primary Bank nor any of its third parties engage in online behavioral tracking. Online behavioral tracking collects personally identifiable information related to a consumers' online activities "over time and across different web sites" through the operator's website or online service.