# Southern Bank of Tennessee
## ONLINE BANKING PRIVACY POLICY NOTICE
## OUR POLICY

The collection, storage and sharing of customer information is an important part of delivering useful banking products and services to consumers. To serve you, as a consumer, efficiently and conveniently, we have to make use of modern technology and customer information. But we know that you are concerned about privacy and our use of the information you give us. We are committed to an ongoing review of our procedures and policies in the interest of protecting your privacy. As a result, we have established the following privacy policy to provide guidance in our dealings with consumers:

## WE RECOGNIZE YOUR EXPECTATION OF PRIVACY

We understand that you expect us to maintain proper safeguards to protect confidential information you provide to us. The privacy of your information is protected not only by state and federal laws but by our commitment to the protection of your financial information. We have established policies and procedures to help prevent misuse of that information. This Policy has been prepared to explain to you what types of information we collect, how we use that information, and the circumstances under which we may share all or part of the information. Under no circumstances do we provide deposit or loan account personal information to third parties for the purpose of independent telemarketing or direct mail marketing of any non-financial products or services of those companies. We disclose information permitted or required by a variety of federal and state laws, as required to consummate your transaction, and as directed by you. Our strict policies to protect your information applies equally to current (active) accounts as well as inactive (closed) accounts both loans and deposits.

For complete details of how we use your information refer to our bank's PRIVACY POLICY. If you have any questions about the use or sharing of consumer financial information or if you wish more information please contact us at **151 E Broad St, Clinton TN 37716 or call 865.457.3433** and we will be happy to answer them. We want to safeguard your trust in us as well as your personal and financial information.

### Your Security and Protection When Online

It is of utmost importance for us to protect your personal information when you are online to our website. We go to great lengths to make sure that your transactions are confidential and secure.

Our Internet Banking System uses a combination of industry-approved security technologies to protect data for the bank and for you, our customers. It features password-controlled system entry, a VeriSign-issued Digital ID for the bank's server, Secure Sockets Layer (SSL) protocol for data encryption, and a firewall to regulate the inflow and outflow of server traffic. To deter users from repeated login attempts, our online system requires the user to key in a Log-In "3 Strikes and your out" mechanism. After three unsuccessful login attempts, the system locks the user out, requiring a phone call to the bank to verify the identity of the user before re-entry into the system. Upon successful login, the Digital ID from VeriSign, authenticates the user's identity and establishes a secure session with that visitor. Once the server session is established, the user and the server are in a secured environment. Because the server has been certified as a 128-bit secure sever by VeriSign, data traveling between the user and the server is encrypted with Secure Sockets Layer (SSL) protocol. With SSL, data then travels between the bank and customer, is encrypted and can only be decrypted with the session key pair. The bank's server issues a public key to the end user's browser and creates a temporary session key. These two keys are the only combination possible for that session. When the session is complete, the keys expire and the whole process starts over when a new end user makes a server connection.

### Encryption, Firewalls, and Other Protection

All requests must pass or filter through a router and firewall before they are permitted to reach our server. A router is a piece of hardware that works in conjunction with the firewall. The firewall is a piece of software that blocks and directs traffic coming into our server. This configuration only allows traffic necessary to process acceptable data requests, such as sending customer requests to the bank or retrieving web pages.

All personal and account information that passes between your computer and Southern Bank of Tennessee Online Banking is encrypted. This means that while your information is in transit, it is scrambled so that only Southern Bank of Tennessee's computer equipment and systems can reassemble it to its original text format. When our bank sends personal account information to you, it is also encrypted so that only your computer can decipher it and reconstruct the data transmitted.

### Your User ID/Password and Privacy of Your Information

The most important way of protecting your Online Banking transactions is by your assigned User ID and self-selected Password. Be sure to keep them a secret. Memorize them and, if you need to maintain a written record of the codes, it is recommended that you store them away from your computer in a secure place and not in your wallet or purse. Always make sure that no one is watching you enter the information and always log off the Southern Bank of Tennessee Online Banking website whenever you are away from your computer (click the log out button). If your computer is left unattended and the browser is running with your User ID and Passwords entered, anyone can gain access to your accounts. It is recommended that you change your Password often and do not use simple words or numbers in sequence. It is required that you use upper case and lower case numbers and letters and use symbols.

It is recommended that you use characters that are unique to you. Stay away from obvious words and numbers, like a family member's birthday or name.

Visitors to our bank's Website remain anonymous. We do not collect identifying information about visitors to our site. We may use standard software to collect non-identifying information about our visitors, such as; (1) Date and time out site was accessed; (2) IP address (A numeric address given to servers connected to the Internet); (3) Web browser used; (4) City, State, and country. If collected, the bank would use this information only to create summary statistics and to determine the level of interest in information available on our site. Visitors may elect to provide us with personal information via E-mail, online registration forms, or our guest book. Any information provided would only be used internally, as appropriate, to handle the sender's request. Information you provide will not be disseminated or sold to other organizations. Some areas of our Website may use a "cookie" temporarily stored in the visitor's computer memory (RAM) to allow the web server to log the pages you use within the site and to know if you have visited the site before.

## Protection and Confidentiality of Nonpublic Personal Information

We are providing this notice as required by the Federal Financial Privacy Law and the Fair Credit Reporting Act.

We limit access to nonpublic customer information about you to our employees who need to know that information for us to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.

Nonpublic personal information means personal financial information about you that we collect in connection with providing you with a financial product or service that is not made publicly available.

## Categories of Nonpublic Personal Information We May Collect

When appropriate in conducting business, we may collect nonpublic information about customers from a variety of sources:
- Information the customer has provided on applications or other forms
- Information about the customer's transactions with us, our affiliates or others
- Information we may obtain from consumer credit reporting agencies
- Information from third parties such as employment verification and property insurance coverage

## Categories of Nonpublic Personal Information We May Disclose

We may disclose nonpublic personal financial information about you to companies that perform marketing services on our behalf or to financial institutions or securities companies with whom we have joint marketing agreements. We will disclose, as permitted by law, but only if directed by you, nonpublic personal information about you to our affiliates(s) or future affiliate(s). These affiliated companies are or will be financial service providers, such as title companies or insurance companies. We may also disclose nonpublic personal financial information about our customers or former customers to non-affiliated third parties as permitted or required by law or authorized by you. We do not sell nonpublic information to telemarketers.

If you no longer do business with us, we will continue to protect your nonpublic personal information using the same policies and practices.

## Frequently Asked Questions

*What are cookies?* - A cookie is a file sent from a website to your computers hard drive that is logged on to the site. This file allows the site to recognize whether the computer has been there before and what security requirements and browser preference the computer requires. Only the site that sent the cookie can read the cookie, and only information that has been given directly by the logged on user to the site is accessible. Computer viruses cannot be transmitted through cookies.

*Do I have to accept cookies?* - You as a customer can choose not to accept cookies. You may do this by making the appropriate selection from your browser options. However, certain services require cookies for effective delivery. Whenever this is the case, you will be informed that you will need to allow cookies if you wish to receive the service. Cookies also make your visit to a site simpler by keeping you from having to re-enter your password every time you change pages within a secure session.