PSB Security Statement

Palmetto State Bank provides Online Banking through Fiserv E-Solutions. E-Solutions requires all of its divisions and companies to take proactive steps to ensure that the systems they own or participate in contain adequate security measures to limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses. State of the art firewall technology is the first line of defense in preventing unauthorized access to any of your account information. Included in the operating system is the capacity to allow only secure connections by end users. Utilizing Secure Socket Layer (SSL) technology, all transmissions of web pages and data between Palmetto State Bank and its customer are completely encrypted and are unreadable to any person or group trying to "intercept" the transmission. SSL encryption is the industry standard and is commonly used in Online applications that require security and privacy for sensitive data.

Online Banking Access ID and Password: To initially access Palmetto State Bank Online Banking you will use an Access ID and Password that our bank assigns to you. The first time you log in you will be required to change your Password. Online instructions will explain Access ID and Password requirements. You will be able to change your password at any time if you feel security has been breached. You agree to keep your Palmetto State Bank Online Banking Access ID and Password confidential to prevent unauthorized access to your accounts and to prevent unauthorized use. For security purposes, we recommend you memorize your Access ID and Password. If you choose to write it down, store it in a secure place. If you violate this agreement and purposely disclose your Access ID and Password to allow others to access your accounts, you are fully responsible for any transactions they make on your accounts.

Data Encryption: When consumers access their account information or any other sensitive data, an encryption system is automatically activated to protect the transmission of information from unauthorized sources. Regardless of the efforts, the Online as a broad-based communication medium when combined with the "open" nature of the Online make it impossible to guarantee absolute confidentiality in all circumstances. However, Palmetto State Bank continues to monitor and review the security procedures that it has in place to protect customer information. These measures are updated as practices change and new technology becomes available.

Customer Responsibilities: When using our Online Banking services you should adhere to the following security features which are designed to help protect the confidentiality of your transactions and account information:

- Never reveal your login ID or password to anyone.
- Never leave your computer unattended during a session.
- When you are finished with an Online Banking session, be sure to LOG OUT (click Exit) before visiting another web site.
- If you cannot close the browser after your Online Banking session, be sure to delete the temporary files stored by the browser on your local hard drive.
- Always report known instances of unauthorized account access when you feel your privacy or security has been violated.
- Never use an e-mail to transmit any personal, business, financial or account information.
- Use the encryption features of your browser.

If you have any questions regarding our Security Statement, or the security of your Online Banking transactions, please contact us at:

Palmetto State Bank
601 1ST Street West 29924
Hampton, SC 29924
Telephone: (803) 943-2671
E-mail: psbanker@palmettostatebank.com