**For Commercial Online Banking Customers**

***Safeguarding Your Information***

At First State Bank of Blakely, the security of customer information is a priority. We are strongly committed to the safety and confidentiality of your records. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public.

**One of the best ways to avoid fraud is to become an educated user.**

**Small- to medium-sized business and government banking accounts are being targeted by criminals every day.**

**Every security system in place today can and has been compromised by criminals. No system that the bank has put in place can catch 100% of fraudulent attempts.**

***** Commercial Accounts and Government Accounts are not covered under Regulation E. *****

***In most circumstances you will be responsible for assuming the loss on fraudulent transactions. It is vital that you follow what are known as "Best Practices" such as:***

- Run summary reports of all transactions to ensure they are accurate.
- Review your transactions the next business day to determine if fraudulent activity has occurred.
- Maintain up to date anti-virus on your computer systems that access financial websites.
- Patch your operating system weekly and ensure that you are updating Java and Adobe applications weekly as well. Vulnerabilities in these applications are utilized by criminals constantly.
- Ideally, dedicate a single PC for online financial transactions and prohibit any other form of web surfing on this PC.
    - Have the firewall specifically restrict access for the workstation to only the IP Addresses of the financial institutions systems. This will prevent individuals from surfing the internet on the PC.
- Do not use passwords that you have also set up at other websites! Always do financial transactions with a password that is not used anywhere else.
- We require a password change every 360 days. However, you can change your password more often than that, and this is a good idea for your own protection.
- Do not utilize common words in your password, such as Password1#.
- Watch out for copycat Web sites that deliberately use a name or Web address very similar to, but not the same as the real one. The intent is to lure you into clicking through to their Web site and giving out your personal information, such as a bank account number, credit card number or Online Banking login information.
    - Therefore, remember that First State's official website address is **http://www.fsbanks.com** and when logging in to our online banking channel, an "s" is added to the "http" to indicate that it is a secure website, so that it reads **https://www.fsbanks.com** By knowing these formats, you can distinguish spoofed or bogus sites that attempt to fool you into thinking you are on our official site.

- Always use your pre-established link to access web sites. Never click on a link contained in an email.
- Pay attention to Security and Balance Alerts transmitted via e-mail or at the login to Online Banking when activity occurs on the account.

**What First State Bank of Blakely does:**

- On at least an annual basis the bank examines its controls that it has implemented for online banking access.
- Based on that review that bank will determine if changes are necessary and will implement required changes on an ongoing basis.
- Reviews the current fraud trends to determine if changes are required in regards to current security controls and provide alerts to our customer base.
- We utilize multi-factor authentication that is in keeping with federal guidelines for online banking.
- We may on occasion call to verify other information regarding your online activity should we see something of concern in your login patterns.
- Once your Online Banking account is set up, all electronic communication is done through the secure email system provided within the online banking system.

**What First State Bank of Blakely does not do, for your protection:**

- We will never ask you for your online banking password.
- We will not contact you via email requesting that you click on a link inside the email.

NOTE: While these layered processes are designed to prevent fraud, they will not catch fraud 100% of the time. You are responsible for losses incurred on commercial and government accounts. Please be vigilant and monitor your account at all times.

In case of errors or questions about your electronic transfers, or any of the Best Practices described above, contact us at your local branch and they will get the ball rolling.