INTERNET SECURITY INFORMATION

Site Security Information
SMB-FA Consumer understands that security and confidentiality are very important to our online customers. That is why we work hard to protect you and your business account information during your online sessions. SMB-FA Consumer is committed to improving your online security and helping protect you against fraud and identity theft while performing online internet banking transactions with SMB-FA Consumer. Your initial level of security and protection is your personally selected User ID, Password and challenge questions & answers to access your account. This initial security check verifies who you are, allowing you access to your account information while helping to prevent unauthorized access.

Cookies
A cookie is a small piece of information which is created by a web server during a user's visit to a web site. If you configure your web browser to alert you regarding the presence of cookies, you may receive a notice that a web server wishes to set a cookie. We may use "transient" cookies -- cookies which are not stored on your hard drive and are not available to anyone other than SMB-FA Consumer. -- in your interactions with our web site. Transient cookies allow you to navigate on our site from one page to another without requiring you to log in again on each page. The transient cookies do not contain any customer-identifiable information and all cookie content is encrypted by use of AES encryption (Advanced Encryption Standard). When you leave our site, or when your session expires, the transient cookies expire.

Security/Fraud Prevention Tips
While SMB-FA Consumer takes precautions to protect the security and confidentiality of your personal and business information, many customers ask what steps they can take to further ensure their account security. Below are recommended tips to help you avoid fraud or identity theft:

- **Log In**
  Protect yourself and your information against fraudulent Web sites by always checking the URL/Address every time you log in. The www.smbfaconsumer.com URL that should appear in your browser contains "www.smbfaconsumer.com".

- **Log Off**
  After you have finished your secured online session, you should always use the Log Out link to end your session. The Log Out link appears on every page in the upper right-hand corner. After you log out, no further transactions can be conducted without re-entering your User ID and password.

- **Create a User ID and Password That Only You Will Know**
  Your User ID and password protect the confidentiality of your account, verify who you are and enable the system to establish your secure session.

  1. Select a User ID and password that are easy for you to remember and difficult for others to guess.
  2. Your User ID and password should be distinctly different.
  3. Try not to use words from the dictionary.

4. Do not use your account numbers as your User ID or password.
5. We recommend that you use a combination of letters and numbers.
6. Memorize your password and never share it with anyone.

- **Change Your Password Frequently**
  Stay ahead of the game and change your password frequently. Simply log in and click on the Change Password link in the navigational bar.

- **Be Aware of Cached Pages**
  Cached pages are pages that are temporarily saved in your computer's memory. You can notice cached pages by clicking on your browser's Back button. While cached pages do not jeopardize the security of your User ID and password, cached pages do retain information submitted. It is best to complete all of your business transactions without leaving the computer and, when finished, log out and close the browser you were using so no one can access previously submitted or viewed information.

- **Beware of Suspicious E-mails or Phone Inquiries**
  Never provide your account number, PIN or password to anyone who calls or contacts you unsolicited. And while SMB-FA Consumer may initiate a contact requesting personal information or security verification, it is good practice to request a callback number to verify that the call is authentic and not someone attempting a fraudulent act.

  If you receive suspicious calls or e-mails claiming to come from SMB-FA Consumer, immediately contact our Customer Service Department at 1-833-624-8400.