



## About Security

Your online security is very important to us. We take several precautions to ensure your information is secure.

To access our secure area, you must enter your Logon ID and Security Code. As a security precaution, we store your Security Code in our database in an encrypted format that even we cannot decode.

In addition, Enhanced Authentication provides extra protection for your online data and helps guard against phishing scams and identity theft by recognizing your computer and usage patterns. If a questionable logon attempt is detected, the system will require additional identity verification before allowing access.

The system also displays a secret Security Phrase that you choose. This phrase is displayed each time you log on to reassure you that you are logging on to your actual Online banking site. If you do not see your Security Phrase, you should not enter your Security Code.

Other online security measures include:

- Automatic time out that occurs if you are inactive in the secure area of our site for more than 10 minutes.
- Use of Extended Validation SSL Certificates – browser bar turns green and displays the name of the organization that owns the website to ensure you are on the site you intended.
- Lock out after 3 unsuccessful attempts at entering the Security Code.
- Secure Sockets Layer (SSL) protocol to ensure that your connection and any information transmitted is protected.
- 128-bit encryption to make your information unreadable as it passes over the Internet.

If your browser does not support SSL or 128-bit encryption, you will need to upgrade your browser.

While we continue to evaluate and implement the latest improvements in Internet security technology, users of the system also have responsibility for the security of their information and should always follow the recommendations listed below:

- Site best viewed and most secure with current versions of Chrome, Firefox, Internet Explorer or Safari.
- Keep your Security Code confidential.
- Be sure others are not watching you enter information on the keyboard when using the system.
- Never leave your computer unattended while logged on to the system. Others may approach your computer and gain access to your account information if you walk away.
- Exit the system when you are finished to properly end your session. Once a session has ended, no further transactions can be processed until you log on to the system again.
- Close your browser when you are finished, so that others cannot view any account information displayed on your computer.
- Keep your computer free of viruses. Use virus protection software to routinely check for a virus on your computer. Never allow a virus to remain on your computer while accessing the system.