

# **Sterling Bank Internet Security**

STERLING BANK is pleased to offer internet banking and bill payment services. Delivering these services requires a solid security framework that protects you and our institution's data from outside intrusion. We are committed to working with our internet service and communications providers to produce the safest operating environment possible for our customers. The information below summarizes our security framework, which incorporates the latest proven technology. A section at the end also summarizes your responsibilities as a user of the internet banking system with regard to security. There are several levels of security within our security framework. User Level deals with cryptography and Secure Sockets Layer (SSL) protocol, and is the first line of defense used by all customers accessing our Banking Server from the public Internet. Server Level focuses on firewalls, filtering routers, and our trusted operating system. Host Level deals specifically with our internet banking and bill payment services, and the processing of secure financial transactions.

## **User Level**

There are several components of User Level security that ensure the confidentiality of information sent across the public Internet. The first requires your use of a fully SSL-compliant 128 bit encrypted browser such as Netscape Navigator or Microsoft Internet Explorer. SSL is an open protocol that allows a user's browser to establish a secure channel for communicating with our Internet server. SSL utilizes highly effective cryptography techniques between your browser and our server to ensure that the information being passed is authentic, cannot be deciphered, and has not been altered en route. SSL also utilizes a digitally signed certificate which ensures that you are truly communicating with the Online Banking Server and not a third party trying to intercept the transaction.

After a secure connection has been established between your browser and our server, you then provide a valid User ID and Security Code to gain access to the services. This information is encrypted, logged by the server forming another complete physical security layer to protect the server's information, and a request to log on to the system is processed. Although SSL utilizes proven cryptography techniques, it is important to protect your User ID and Security Code from others. You must follow the Security Code parameters we specify at the time you

sign up for an Internet banking account. We also recommend changing your Security code often. Session time-outs and a limit on the number of logon attempts are examples of other security measures in place to ensure that inappropriate activity is prohibited at the User Level.

## **Server Level**

All transactions sent to our Banking Server must first pass through a filtering router system. These filtering routers automatically direct the request to the appropriate server after ensuring the access type is through a secured browser and nothing else. The routers verify the source and destination of each network packet, and manage the authorization process of letting packets through. The filtering routers also prohibit all other types of Internet access methods at this point. This process blocks all non-secured activity and defends against inappropriate access to the server.

The Banking Server is protected using the latest firewall platform. This platform defends against system intrusions and effectively isolates all but approved customer financial requests. The platform secures the hardware running the Online applications and prevents associated attacks against all systems connected to the Banking Server. The system is monitored 24 hours a day, seven days a week for a wide range of anomalies to determine if attempts are being made to breach our security framework.

## **Host Level**

Once authenticated, the customer is allowed to process authorized internet banking and bill payment transactions using host data. In addition, communication time-outs ensure that the request is received, processed, and delivered within a given time frame. Any outside attempt to delay or alter the process will fail. Further password encryption techniques are implemented at the host level, as well as additional security logging and another complete physical security layer to protect the host information itself.

## **User Responsibilities**

While our service provider continues to evaluate and implement the latest improvements in Internet security technology, users of the online banking system also have responsibility for the security of their information and should always follow the recommendations listed below:

- Utilize the latest 128 bit encryption version of either Netscape Navigator or Microsoft Internet Explorer. The online banking system is best viewed and is most secure when you use one of these two browsers, as they are both certified for use at our site.
- Your Security Code must be kept confidential. You must follow our specific parameters for a Security Code and change it frequently to ensure that the information cannot be guessed or used by others.
- 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 online banking system. Others may approach your computer and gain access to your account information if you walk away.
- Click Exit when you are finished using the system to properly end your session. Once a session has been 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 online banking system.
- Report all crimes to law enforcement officials immediately.

When you follow these simple security measures, your interaction with the online banking system will be completely confidential. We look forward to serving your online banking and bill payment needs both today and into the future - securely!