# CLARKE COUNTY STATE BANK
# ONLINE SECURITY STATEMENT

## Security Statement

The Internet Banking System brings together a combination of industry-approved security technologies to protect data for the bank and for you, our customer. It features password-controlled system entry, a VeriSign Class 3 encryption certificate for the bank's server, and a Secure Sockets Layer (SSL) protocol for data encryption.

## Secure Access and Verifying User Authenticity

The Internet Banking System requires multi-factor authentication which involves a specific security key, random generated code, and security questions to register a computer to access internet banking. To begin a session with the bank's server the user must key in a user name and a random code. Next the user must answer a security question. Finally, the user must enter their password with their assigned security key. Our Internet Banking System uses a "3 strikes and you're out" lockout mechanism to deter users from repeated login attempts. After three unsuccessful login attempts, the system locks the user out, requiring a phone call to the bank to unlock the user before re-entry into the system. Upon successful login, the digital ID from VeriSign, the experts in digital identification certificates, authenticates the user's identity and establishes a secure session with that visitor.

Mobile Banking utilizes the same security layers as Internet Banking plus registers the device in the Cavion program. The device can then be blocked from submitting any transactions.

## Secure Data Transfer

Once the server session is established, the user and the server are in a secured environment. Because the server has been certified as a 128-bit secure server by VeriSign, data traveling between the user and the server is encrypted with Secure Sockets Layer (SSL) protocol. With SSL, data that travels between the bank and customer is encrypted and can only be decrypted with the public and private key pair. In short, the bank's server issues a public key to the end user's browser and creates a temporary private key. These two keys are the only combination possible for that session. When the session is complete, the keys expire and the whole process starts over when a new end user makes a server session.

## Physical and Other Security

Monitored firewalls, intrusion detection systems and other solutions protect e-mail servers and web hosting servers from the internet. The data centers are located in secure, continually monitored facilities with an electronic passkey and biometric access. The data centers have a raised-floor design and are protected by waterless fire suppression system and redundant HVAC and uninterruptible power supply backups as well as alternate power sources.

Using the above technologies, your Internet banking transactions are secure.