

Security Statement

State Bank of Alcester provides Internet Banking & Bill Pay access through Information Technology, Inc. (ITI). ITI requires all of their divisions and companies to take proactive steps to ensure that the systems they own or participate in contain adequate security measures to limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses. The Internet Banking & Bill Pay services run on a Windows 2003 Server operating system. State of the art firewall technology is the first line of defense in preventing unauthorized access to any information housed.

Included in this operating system is the capacity to allow only secure connections by end users. Utilizing Secure Socket Layer (SSL) technology, all transmissions of web pages and data between the financial institution and its customer are completely encrypted and are unreadable to any person or group trying to "intercept" the transmission. SSL encryption is the industry standard and is commonly used in Internet applications that require security and privacy for sensitive data.

Multi-Factor Authentication: Each time consumers access the service, they will be asked to enter their Access IDs. After they enter their Access IDs on a registered computer, they will be shown the Authentication Image and Authentication Pass Phrase they have chosen. If they do not see the Authentication Image and Authentication Pass Phrase they have chosen, they should not enter your password and are responsible for calling the bank immediately to report the problem. If they see the Authentication Image and Authentication Pass Phrase they have chosen, they can enter their passwords and click "Submit." They will then have access to the service.

After they enter their Access IDs on a non-registered computer, they can choose to answer a Challenge Question or get a one-time Passcode emailed to the address in the bank's records. They must either answer the Challenge Question or enter the one-time Passcode to access their accounts. The correct responses will allow them to view an Authentication Image and Authentication Pass Phrase. If they see the Authentication Image and Authentication Pass Phrase they have chosen, they can enter their passwords and click "Submit." They will then have access to the service.

Without the proper login, individuals cannot see or use any web pages within the E-Banking product.

Account Number Masking and Account Aliases: When the account number needs to be displayed, it may appear as ###456789 instead of 123456789. Account "Nicknames" are user-defined titles for the consumer's account (i.e., "My Checking") and is used when displaying account information on the screen.

Secure Connection: When consumers are accessing the online information, their connection is automatically converted into a secure Internet communications session.

Data Encryption: When consumers access their account information or any other sensitive data, an encryption system is automatically activated to protect the transmission of information from unauthorized sources.

Regardless of the efforts, the relative infancy of the Internet as a broad-based communication medium when combined with the "open" nature of the Internet make it impossible to guarantee absolute confidentiality in all circumstances. However, State Bank of Alcester continues to monitor and review the security procedures that it has in place to protect customer information. These measures are updated as practices change and new technology becomes available.

If you have any questions regarding these policies and procedures, please contact us ([link to contact page](#)).