

Landmark Community Bank provides Internet banking (E-Banking) access through Jack Henry and Associates' NetTeller service. Jack Henry and Associates requires all of its 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 Service Bureau runs on a robust Windows 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. Secure Socket Layer (SSL) technology encrypts all transmissions of web pages and data between the financial institution and its customers and renders unreadable customer information 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.

Passwords: Before the customer accesses Internet Banking, they are required to enter their user ID and password. Without the proper login, individuals cannot see or use any web pages within the E-Banking product.

Account Number Masking and Account Aliases: For security reasons, complete account number(s) never appear on the computer screen. When the account number needs to be displayed it appears as #####6789 instead of 123456789. Financial institutions have the flexibility to determine how many digits are "unmasked" and the masking will always occur from the left. Account "aliases" are user-defined titles for the customer account (i.e., "My Checking") and is used when displaying account information on the screen.

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

Data Encryption: When customers access their account information or any other sensitive data, an encryption system is automatically activated to protect the transmission of information from unauthorized sources. 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, "Financial Institution" continues to monitor and review security procedures 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 at: 901.850.0555.