ONLINE SECURITY STATEMENT

What We Do

Legacy Bank works hard to provide you with a secure online experience that protects your confidential information. We safeguard information according to industry-accepted security standards and procedures, and we continually assess new technology for protecting information. Our security measures include the following:

Access ID and Password

Access to your account information via our online banking service is possible only with your valid access ID and password. User IDs and passwords are isolated from the Internet by being stored on secured computer systems. The online banking system automatically disallows a user after three invalid attempts.

Multifactor Authentication

An additional layer of security and fraud protection has been added to help prevent identity theft. When you sign up for online banking you will be required to establish an authentication image and pass phrase and three security challenge questions. Your authentication image and pass phrase will help to confirm that the website you are visiting is authentic and your security challenge questions will serve as a second layer of security to verify your identity on non-registered computers.

Encryption

Our system ensures that data exchanged between your PC and our computer networks are encrypted with 128-bit encryption – the strongest encryption available. Encryption is accomplished through Secure Socket Layer (SSL) technology which utilizes mathematical formulas to "encrypt" or hide information from prying eyes on the Internet. Additionally, if SSL detects that data was added or deleted after you sent it to the Bank, the connection will be severed in order to guard against any tampering. The most popular browsers have the SSL security feature included. If you see a website address that begins with "https" (as opposed to "http") and the "closed lock" icon in the window of your website browser, you are using an SSL connection to transfer your confidential information.

Firewalls

To protect data stored on our systems and to help prevent unauthorized access, we employ firewalls where appropriate. Firewalls are software and hardware products that designate parameters, and control and limit the access outside computers have to the Bank's internal networks and data bases.

Automated Time Out

To provide additional protection, a time out feature is used on selected portions of our website. This feature will automatically log you off of your current online session after a period of inactivity. Re-establishing and authenticating your credentials for your online session helps to reduce unauthorized access to your accounts.

Third-Party Verification

The Bank works with independent third-party security firms to perform security reviews of our online services and systems. Systems are monitored and updated as needed to protect against known security risks. In addition, the website is also registered with VeriSign, an industry leader in website identification and encryption. Via your browser, VeriSign allows you to confirm this website provider's identity before transmitting any personal information.

Linking to Third Party Websites

On occasion, Legacy Bank may provide access to information, products or services offered on websites operated by third parties. We provide this access through the use of hyperlinks that automatically move you from the Legacy Bank website to the third party website. When you visit a third party website by using a link on Legacy's website, you will no longer be protected by Legacy Bank's privacy policy or security practices. The data collection, use and protection practices of the third party website may differ significantly from the practices of the Legacy site. Legacy Bank does not guarantee and is not responsible for the privacy or security of these websites. Also, while we do our best to provide you with helpful, trustworthy resources, we cannot endorse, approve or guarantee information, products, services or recommendations provided at any third party website.

Cookies

Cookies are electronic files that your Internet browser places on your hard drive to retain information relating to visits to and use of a website. We use cookies to improve the functionality of our site. We do not use cookies to store or transmit personal information. We use cookies to enable our customers to navigate more easily within our site during an online session. We use "persistent" cookies to allow you to set and maintain your preferences for using our site. Persistent cookies remain on your computer's memory after you close your Internet browser.

You can block cookies by changing the setting on your Internet browser or through the use of software programs specifically designed to block cookies. Note, however, that if you choose to block cookies, you will not be able to log into our secure online banking service and you may limit other functionality we can provide when you visit our site. You can also remove cookies by deleting them from your temporary Internet or cookies folder.

Children's Online Privacy

This website is not directed to children. We do not market to children, nor do we knowingly collect or retain personally identifiable information from children. Visit the Federal Trade Commission website for more information about the Children's Online Privacy Protection Act (COPPA).

What You Can Do

Legacy Bank takes the safeguarding of your information seriously. However, we understand that the protection of your sensitive information does not start and stop with Legacy Bank. Security is everyone's responsibility; you are our most important partner in creating a safe and secure banking environment. While we can take several precautions to protect your private information, you have the responsibility of protecting yourself from fraud and identity theft. Here are some steps you can take to improve your level of personal security:

Basic security - Keep your user ID, password, account numbers, personal identification numbers and other account data confidential. Change your password regularly and choose one that is difficult to guess. Make it a regular habit to log out of online banking when you're finished. Clear the browser's cached pages and history before leaving a shared or public computer.

Virus management - Install and update virus protection software to reduce the risk of viruses getting into your computer. Use extreme caution when opening email received from unknown sources and pay special attention to any attachments.

PC software - Ensure your browser is using the highest encryption available. Legacy Bank currently requires 128-bit encryption. Install software only from trusted sources and known origins.

Communicating with others - Use good judgment in communication with others, especially those you do not know. Regular non-encrypted Internet email is not secure. Use caution when reviewing privacy policies and acceptance terms for online products and services.

Account management - routinely review and reconcile your account information. Notify us immediately at 561-544-8400 if you believe there has been an unauthorized transaction in your account or you believe the security of your password has been compromised.