

Internet Banking Security Statement

With Business Connect Internet Banking, we use a full range of Internet security measures, including cryptography, routers and firewalls, and a trusted operating system to complete our overall security architecture.

Cryptography

Security on the Internet begins with your browser. In order to utilize Business Connect Internet Banking, you must use a browser that supports the Secure Sockets Layer (SSL) protocol. SSL allows you to securely send and receive encrypted data over the Internet. This protocol provides a secure channel for data transmission through its public/private key encryption capabilities. When you connect to the Internet Banking Vault Server, the session immediately goes through a "handshaking" process where the server sends a certified Digital ID to you, whereupon an "encrypted tunnel" is created between you and the server. This simply means that all requests by you and, subsequently, all replies by the server are encrypted using an extremely long and complicated key.

We recommend the following browser:

- Microsoft Internet Explorer 7.x

We support the following browsers:

- Firefox 3 and higher
- Safari 1 and higher

If you are not using one of the supported browsers:

You may experience issues with Internet Banking. If this occurs, please download one of the browsers listed and attempt the action again.

Can I use a Beta version of one of the Browsers above?

We do not recommend using a Beta version of any browser. When new versions of browsers are fully tested and deemed compatible with the Internet Banking product, they will be updated on the supported browsers list.

The following types of browsers and tools are not recommended or supported for use with Internet Banking:

- Embedded Browsers contained within Personal or Commercial Financial Management Software (Quicken, Quickbooks, Money, etc.)
- Browser Add-Ins and Toolbars (IE 7 Pro, Google, Yahoo, etc.)

If you are using a non-supported browser, an embedded browser or a browser add-in, you may experience functionality issues with Internet Banking. If this occurs, please download one of the browsers listed above or remove the add-in and attempt the action again.

Routers and Firewalls

Account information is protected by a series of filtering routers and firewalls that act as a barrier between the outside world and the internal bank network. The filtering router is the first component that you would pass through to gain access to your account information. Much like a security guard, the router is responsible for determining who has access to what components of Internet Banking. This is achieved with Access Control Lists (ACLs) which allow or deny specific services for a particular user.

The firewall is the next security component that you would pass through. The firewall provides a higher level of security and authentication of a customer request. The firewall takes advantage of the same type of ACLs that a router utilizes and tracks each request that was made, who made it, when it was made, where it was made from, and where it was destined. Each one of these items is used to determine whether the user is granted access to the requested destination and protects the internal bank network from outside access.

Trusted Operating System

The entire Internet Banking application resides within a trusted operating system. The trusted operating system acts much like a firewall by protecting sensitive and proprietary information from the outside world. The trusted operating system accepts your authorized requests for account information, retrieves the information from our database, and sends the information back to your browser in an encrypted format. The system also contains numerous audit controls to track requests and navigation. This audit control allows us to quickly identify any suspicious activity.

Your Responsibility

When an Internet Banking account is established, we will provide you with a username and password to access your accounts through the Internet. The

first time you attempt to access your account, you will be prompted to change your password. It is important that you memorize your password and not convey it to anyone else. You must make sure that no one is watching as you enter your password and that you properly exit the Internet Banking session/browser before leaving the computer. The Internet Banking system allows you to change your password anytime and you should change your password frequently.