Bank of St. Croix, a Division of United Fidelity Bank, fsb (Bank of St. Croix) is pleased to offer Online Banking, including but not limited to Personal Online Banking, Business Banking Online, and Online Bill Pay. Delivering these services requires a solid security framework that protects data from outside intrusion. Bank of St. Croix is committed to providing the safest operating environment possible for our customers. The information below summarizes our security framework, which incorporates the latest proven technology.

User Level security ensures the confidentiality of information sent across the public Internet. You are required to use a fully (Secure Sockets Layer) SSL-compliant 128 bit encrypted browser such as Mozilla Firefox or Microsoft Internet Explorer. SSL allows a user's browser to establish a secure channel for communicating with our Internet server. SSL utilizes highly effective cryptography techniques between your browser and our server to ensure that the information being passed is authentic, cannot be deciphered, and has not been altered. SSL also utilizes a digitally signed certificate which ensures that you are truly communicating with the Internet Banking server and not a third party trying to intercept the transaction.

After a secure connection has been established between your browser and our server, you then provide a valid Access ID and Password to gain access to the services. This information is also encrypted. Although SSL utilizes proven cryptography techniques, it is important to protect your Access ID and Password from others. You must follow the Access ID and Password parameters we specify at the time you sign up for Online Banking. We also recommend changing your Password periodically. Session time-outs and a limit on the number of logon attempts are examples of other security measures in place to ensure that inappropriate activity is prohibited at the User Level.

The Banking Server is protected using the latest firewall platform. This platform defends against system intrusions and effectively isolates all but approved customer financial requests. The platform secures the hardware running Online Banking and prevents associated attacks against all systems connected to the Banking Server. The system is monitored 24-hours a day, seven days a week for a wide range of anomalies to determine if attempts are being made to breach our security framework.

Once authenticated, the customer is allowed to process authorized Online Banking transactions using host data. In addition, communication time-outs ensure that the request is received, processed, and delivered within a given time frame. Any outside attempt to delay or alter the process will fail. Further password encryption techniques are implemented at the host level, as well as additional security logging and another complete physical security layer to protect the host information itself.