ONLINE BANKING SYSTEM SECURITY

In Internet banking as with traditional banking methods, security is a primary concern. At Bank of Commerce we have taken every precaution necessary to be sure your information is transmitted safely and securely. The latest methods in Internet banking system security are used to increase and monitor the integrity and security of the system.

The security of the Bank of Commerce Internet banking application is addressed at three levels. The first concern is the security of customer information as it is sent from the customer's PC to the Web server. The second area concerns the security of the environment in which the Internet banking server and customer information database reside. Finally, security measures are in place to prevent unauthorized users from attempting to log into the online banking section of the Web site.

Data security between the customer browser and our Web server is handled through a security protocol called Secure Sockets Layer (SSL). SSL provides data encryption, server authentication, and message integrity for a Internet connection. In addition, SSL provides a security "handshake" that is used to initiate the connection. This handshake results in the client and server agreeing on the level of security they will use and fulfills any authentication requirements for the connection. Currently Bank of Commerce's online banking application supports data encryption at the highest level (128 bit). In order to get this level of encryption, you will need a modern browser.

Requests for online banking information are passed on from the Web server to the Internet banking server. The Internet banking application is designed using a three-tiered architecture. The three-tiered architecture provides a double firewall, completely isolating the Web server from the customer information SQL database.

The World Wide Web interface receives SSL input and sends requests through a firewall over a dedicated private network to the Internet banking server. The World Wide Web interface is the only process capable of communicating through the firewall to the Internet banking server. Therefore, only authenticated requests communicate with the Internet banking server.

The customer information database is housed on a Microsoft SQL Server, which implements Microsoft NT security in addition to the firewall technology. The customer database is stored on a RAID-5 drive array, which provides uninterruptible data access, even in the event of a hard drive failure. Just as the World Wide Web interface is the only process capable of communicating with the Internet banking server, the Internet banking server is the only process able to send requests to the SQL database. Thus, the outside world is removed from the customer database by two dedicated private networks.

A security analyzer constantly monitors login attempts and recognizes failures that could indicate a possible unauthorized attempt to log into an account. When such trends are observed, steps will be taken automatically to prevent that account from being used.

Security concerns have been addressed from every angle within the architecture of the Internet banking application. Implementation of the SSL security protocol on the Web server and customer browser ensures authenticated data has been received from the customer. The three-tiered approach of the Internet banking application creates a double firewall which performs information requests over dedicated networks designed to handle specific functions. Placing all business logic and event logging within the Internet banking server creates a controlled environment which allows quick incorporation of Internet security technologies as they evolve. Finally, the security analyzer monitors login attempts in order to prevent unauthorized logins.