

## **Direct+ Security Statement**

The Direct+ architecture includes security on multiple levels. End users access the application through a Secure Sockets Layer (SSL) connection. A single sign-on capability is provided to authenticate the user's credentials and provide the applications with information regarding activities the user is authorized to perform.

End user authentication is implemented within the architecture using passwords or, in the case of sensitive transactions, multi-factor authentication provided via RSA tokens. Network-based security controls are employed to protect and isolate sensitive system components. Encryption technology is used to secure data in transport between components.