RBA Web-Based Applications Security

In addition to using industry standard SSL/TLS encryption, our web-based applications are hardened against many different attack vectors, to ensure that sensitive information remains safe from hacking attempts. The software protects against exploitation via:

- **SQL Injection**
  - Uses object-relational (O/R) mapping technology which generates parameterized queries for all data access.
- **Cross-site scripting (XSS)**
  - Performs input validation in both client and server code, preventing malicious scripts from circumventing client-only validation and entering invalid data.
- **Unauthorized access to application**
  - Primary firewall prevents all connections except HTTPS web traffic from reaching the public web server.
  - Passwords are never stored "in the clear;" instead, they are 'salted' and cryptographically hashed.
  - In order to change ownership of an account on the system, users must visit a one-time-use link sent through email and confirm current password.
  - The system utilizes 'Captcha' entry to discourage automated submissions by a malicious script or program.
- **Unauthorized access to private database**
  - A second firewall prevents any direct Internet communication to the private SQL database server.
  - Only SQL database communication is allowed between the public application web server and private SQL database server.
  - The connection string and login credentials used by the RBA application to communicate with the SQL database server are encrypted, so an attacker cannot connect to the database, even in the unlikely event of a public web server breach.
- **Reverse engineering**
  - RBA application source code is protected from decompilation through use of enterprise-grade obfuscation technology.