# Wealth Management System Security

The security of your data is our top priority. That's why we've designed a system with state-of-the-art technology and processes to protect your data 24 hours a day, 7 days a week. We combine world-class technology, with the best data storage facilities and lockdown privacy to bring you a system where you can have peace of mind.

### Our system is non-transactional.

- This makes it impossible for money to be moved in or out of the system.
- It is therefore unlike online banking, online shopping or bill pay where money can be moved.

### Data is stored at SunGard Data Systems.

- SunGard is a revolutionary Internet server hosting space that is the most secure environment available in the industry, offering software or processing solutions for $15 trillion in investment assets worldwide daily.
- SunGard's world-class Hosting Centers protect and support our mission-critical servers and applications.
- Physical access at SunGard is limited to authorized personnel, and requires multiple levels of authentication, including fingerprint scanning.
- SunGard's services include: fire protection and electronic shielding, redundant Internet access, 24 x 7 monitoring and database backups.
- SunGard helps ensure uninterrupted service and the highest levels of performance, security and reliability.

### Data is secured behind firewalls.

- A firewall is a security device that creates a barrier between the Internet and computing equipment and applications.
- Firewalls block unauthorized data access. If an incoming packet of information is flagged, it is not allowed to enter the system.
- An additional layer of protection is created by also trafficking data from the application server to the database server through the firewall.

# Security Information

### Our password protected system can only be accessed by valid users.

- Each User has a unique User Name and Password.
- If three consecutive, incorrect login attempts are made, the system automatically locks the account for a period of 10 minutes, rendering manual or programmatic hacking attempts ineffective.
- If the account is accidentally locked or a password forgotten, the "forgot password" button can be selected on the login screen and a temporary password will be sent to the registered email address.
- User IDs and Passwords are never given out over the phone or sent to email addresses that are not pre-registered with the account. No one has access to an individual's password unless they supply it.
- As added protection for financial information, the system can instruct the user's browser to not store any financial information on the user's computer.

### Designated as a VeriSign Secure Site.

- All information is routed through Secure Socket Layer (SSL), which creates an encrypted connection between the browser and the web servers.
- The application cannot be accessed through an unsecure connection. It uses 256 bit encryption, the latest and most secure available today.

### Certified Hacker Safe.

- Hackersafe approval means our ASP-based system is updated every 15 minutes with tests for newly discovered vulnerabilities and validated fixes from hundreds of sources worldwide.
- The system meets the highest published government standards.

### The system uses Watchfire's AppScan Technology.

- During development test situations are simulated and potential vulnerabilities identified so they can be eliminated before public release.

### It supports 256 bit encryption with current browser technology.

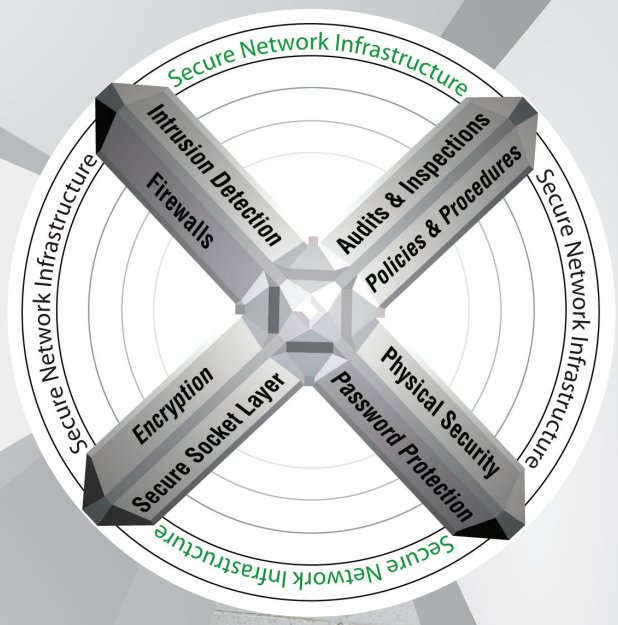
- Encrypted information is simply scrambled data. Once scrambled, the data can only be read after it has been decrypted. Decryption mathematically unscrambles the information using a secure session "Key".
- To date no one has been able to crack 128 bit encrypted data let alone 256 bit encryption. This advanced level of encryption uses a special algorithm making the code a trillion times stronger.

### A Security (and Incident) Response Team is maintained.

- The team members, from the executive staff, operations, customer service and technology and development groups each has their own responsibilities to help ensure system security.

**The entire production network is automatically monitored and policed for intrusion attempts 24 hours a day, 7 days a week, 365 days a year.**

- All servers, including the firewalls, are protected by intrusion detection software within the network infrastructure.
- Any recorded intrusion attempts would be analyzed to determine the identity of the intruders and the extent of the intrusion.
- If unauthorized server access was detected the software would sound an alarm and notify operation's staff.
- The Secure Network Infrastructure is regularly audited and inspected to ensure that the security tools utilized are up to date.



The security
of your data is
our top priority.

©eMA-20111130