Our Security Practices

With regard to the security of your personal information, we employ a variety of electronic, physical, and procedural safeguards to protect your personal information including:

Encryption - We employ 128-bit Secure Sockets Layer (SSL) technology to encrypt your personal information when it is in transit between your web browser and our web server or vice versa. In addition, we also use advanced encryption when storing or backing up your personal information on our computers, substantially reducing the risk even in the event of loss or misuse of your personal information.

Software and Hardware Security - We employ stringent, up-to-date software and hardware solutions to minimize the risk that your encrypted, personal information could be hacked, lost, or stolen from our computer systems.

Physical Security - Your encrypted, personal information is located and stored in secure areas within our building and any offsite data processing facilities.

Access - Access to your personal information (either physically or online) is limited to you and our employees who have a "need to know" in order to perform their jobs and who have the appropriate authentications such as key cards, user IDs, and passwords. A user ID and password is required on the Sign In page on our web site for you to access and/or update your account information. Please remember to keep your user id and password secure. Also, if you prefer additional security, we offer our AccountLock feature which will prevent access to your account even with a valid user id and password. Access will only be granted after you request a pass code from us. We will then email you a randomly-generated, temporarily available pass code, allowing you one-time access to your account.

Training - We provide training to our employees regarding our security procedures.