

The following measures are in place to maintain the security of your account:

- **Customer ID/Username and Password** — We require that you enter a customer ID/username and password to enter the secure account section of our website. If you are unable to provide a correct customer ID/username or password, you will be referred to our Customer Contact Center through a toll-free phone number. We encourage you to create a hard-to-guess password, and we recommend that you do not reveal your password to anyone. For added security, your ID/username and password text will be cleared from your Web browser as soon as you leave the website sign-in page.
- **128-Bit Encryption** — We utilize some of the strongest commercially available encryption methods. When you access your account and perform transactions on our website, your information is protected by "128-bit encryption" so that your transactions are safe and secure. Encryption technology establishes a secure connection from the point it leaves your device until it enters our Web servers. Encryption helps ensure that your data cannot be intercepted while in transit.
- **Date/Time Stamp** — Every time you sign in to your account, we display the date and time of your last visit. Contact us if you suspect that the date and time do not match the last time you accessed your account.
- **Secure Firewalls** — All of our computer systems are protected by numerous firewalls to help prevent unauthorized access to our network. Our security personnel monitor these firewalls 24 hours a day, seven days a week to prevent unauthorized intrusions and security breaches.
- **Session Timeouts** — If you're signed in and not using the secure account section of our website for an extended period of time, your session will automatically "time out" and log you off. To resume your activity, you will need to re-enter your customer ID/username and password.
- **Monitoring** — We monitor online access to account information to preserve all information necessary to validate data transmission and to guard against discrepancies or exceptions. If an activity is deemed suspicious, we will take appropriate action, including notifying you for verification.
- **Secure Message Center** — You can have account-related questions answered securely and privately through our Customer Contact Center.

To enhance your browsing experience and for optimal performance when connecting to our website, we recommend you use Microsoft® Internet Explorer 7.0 or above, Firefox 3.6 or above, Google Chrome, or Safari 4.0 or above (for Mac).

You can help protect yourself by keeping your operating system, browser, and antivirus software up to date. Before entering any sensitive information, be sure you see the letter "s" at the end of "http" ("https") in your browser's address bar. This indicates that the data are encrypted and the site is secure. Note that all pages within this site (after sign-in) are secure, but others we link to may not be.

Protect Yourself from Identity Theft - Identity theft occurs when someone wrongfully obtains and uses another person's personal information to take on that person's identity. To learn more about identity theft and reduce your online risk, **[click here](#)**.

In addition, we will monitor relevant developments and advances in Internet security technology and make appropriate enhancements to our security measures where necessary.