Security & Fraud

We are committed to protecting the security of your personal information. We list some activities below that we perform in order to safeguard your data and some tips that you can follow to protect your security.

What We Do:

- We employ industry-proven standards and technologies to protect information in our computing environment.
- We protect our systems and networks from the Internet with firewall systems.
- We use the latest encryption technology with a Digital Certificate issued by an industry leading Certificate Authority to protect sensitive information that is transmitted over the Internet.
- We control access to your information inside our company by limiting employee access to systems and data.

What You Should Do:

- Protect your Username and Password. Avoid choosing easily guessed words or numbers. Avoid writing your sign in information in a place where others can view it.
- Use the 'Sign Out' button to sign out from Online Account Access upon completion of your session and close your browser.
- Do not use email for account-specific questions. Email is not normally encrypted and your account information could be intercepted.
- Review your statement information regularly for unauthorized transactions.

Alerts Regarding Phishing and Web-Spoofing:

- Phishing is an Internet scam (spoof) in the form of an email or pop-up box. The emails and pop-ups link to sites that look like well-known legitimate businesses and ask you to provide and confirm personal, financial, or password information.

- Legitimate businesses do not ask for this information unless you initiate a request for a service. Please DO NOT RESPOND to these emails requesting personal identity, accounts or password information.
- Scam emails often contain misspelled words, poor grammar, awkward or unprofessional writing and typos.
- Be suspicious of urgent or alarming appeals that request security information.

Fraud Alerts:

- Credit One Fraud Alerts messages are provided to you at no cost. You will not be charged for alerts received.
- Message frequency varies, as they are only sent when there is suspicion of fraud.
- Mobile carriers are not liable for delayed or undelivered messages.
- For help send HELP to 89283.
- Send STOP to 89283 to end future fraud alert messages.
- For support contact us at 1-877-825-3242.

To learn other ways to avoid email scams and deal with deceptive spam visit the Federal Trade Commission site at www.ftc.gov/spam