Identity theft has become a major issue in the United States and throughout the world. Below is some information with respect to online identity theft and security reminders that may help you reduce this serious risk.

How Online Identity Theft Can Happen

- Many identity thieves use malicious software programs to attack vulnerable computers of online users. These software programs can monitor your computer activity and send information back to the thief's computer. Sometimes, these programs will log your keystrokes, which allows identity thieves to easily obtain username and password information for any of your online accounts, including your brokerage or other financial or investment accounts.
- Other identity thieves "phish" for your personal information. "Phishing" involves the use of fraudulent emails and copy-cat websites to trick you into revealing valuable personal information, such as your account number, your social security number, and the username and password information you use when accessing your account. Sometimes fraudsters will use phishing scams to try to get you to download keystroke logging or other malicious software programs unsuspectingly.
- But not all identity thieves have gone "high tech." Many still use less sophisticated ways of stealing your personal information, such as looking over your shoulder when you're typing sensitive information, searching through your trash for confidential account information, or extracting personal information about you in a phone call.

How to Protect Yourself Online

You need to protect yourself against identity thieves, whether hackers, phishers, snoops or conmen, when you use your online accounts and services. Here are a few suggestions on ways to keep your personal information and money more secure when you go online:

Beef Up Your Security. Personal firewalls and security software packages (with anti-virus, anti-spam, and spyware detection features) are a must-have for those who engage in online financial, investment and trade transactions. Make sure your computer has the latest security patches, and make sure that you access your account only on a secure web page using encryption. The website address of a secure website connection starts with "https" instead of just "http" and has a key or closed padlock in the status bar (which often appears in the lower right-hand corner of your screen).

Security Tip: Even if a web page starts with "https" and contains a key or closed padlock, it's still possible that it may not be secure. Some phishers, for example, make spoofed websites which appear to have padlocks. To double-check, click on the padlock icon on the status bar to see the security certificate for the site. Following the "Issued to" in the pop-up window you should see the name matching the site you think you're on. If the name differs, you are probably on a spoofed site.

Enable Two-Step Verification for online access to your account. Some online service providers require two-step verification (also called multi-factor authentication or 2FA, each time you login, or on other frequent bases. Some online service providers do not require 2FA but offer it to you as an option or choice. If so, you, should enable this security feature to add an extra layer of protection when accessing your online accounts and services, including the ones you have with TradeStation. With 2FA, you will be required to provide two factors or means of authentication when you log in.

Be Careful What You Download. When you download a program or file from an unknown source, you risk loading malicious software programs on your computer. Fraudsters often hide these programs within seemingly benign applications. Think twice before you click on a pop-up advertisement or download a "free" game or gadget.

Use Your Own Computer. It's generally safer to access your online accounts from your own computer than from other computers. If you use a computer other than your own, for example, you won't know if it contains viruses or spyware. If you do use another computer, be sure to delete all of the your "Temporary Internet Files" and clear all of your "History" after you log off your account.

Don't Respond to Emails Requesting Personal Information. Neither a TradeStation Group company, nor any other legitimate entity, will ask you to provide or verify sensitive information through a nonsecure means, such as email. If you have reason to believe that a TradeStation Group company or any other financial institution actually does need personal information from you, pick up the phone and call the company yourself - using the number in your own records, not the one the email provides.

Security Tip: Even though a web address in an email may look legitimate, fraudsters can mask the true destination. Rather than merely clicking on a link provided in an email, type the correct web address into your browser yourself (or use a bookmark you previously created).

Be Smart About Your Password. The best passwords are ones that are difficult to guess. Try using a password that consists of a combination of numbers, letters (both upper case and lower case), punctuation, and special characters. You should change your password regularly and consider using a different password for each of your online accounts. Don't share your password with others and never reply to phishing emails with your password or other sensitive information. You also should not store your password on your computer. If you need to write down your password, store it in a secure, private place.

Use Extra Caution with Wireless Connections. Wireless networks may not provide as much security as wired internet connections. In fact, many "hotspots" – wireless networks in public areas like airports, hotels and restaurants – reduce their security so it's easier for individuals to access and use these wireless networks. Unless you use a security token, you may decide that accessing your online accounts through a wireless connection isn't worth the security risk.

Log Out Completely. Closing or minimizing your browser or typing in a new web address when you are finished using your online account may not be enough to prevent others from gaining access to your account information. Instead, click on the "log out" button to terminate your online session. In addition,

you should not permit your browser to "remember" your username and password information. If this browser feature is active, anyone using your computer will have access to your brokerage account information.

TradeStation Securities, Inc., ***TradeStation Crypto, Inc***., and ***TradeStation Technologies, Inc.*** are each wholly owned subsidiaries of ***TradeStation Group, Inc.***, all operating, and providing products and services, under the *TradeStation* brand and trademark. ***You Can Trade, Inc.*** is also a wholly owned subsidiary of ***TradeStation Group, Inc***., operating under its own brand and trademarks.