CONCOURSE FINANCIAL GROUP SECURITIES (CONCOURSE)
ONLINE SECURITY DISCLOSURE

In an age of frequent cyber-attacks, phishing attempts, and other online security threats, it is important to always remain vigilant. Check your accounts often and review your credit report at least annually. You are entitled to one free copy of your credit report every year from each of the three nationwide credit reporting companies.

Call Concourse Client Services at 800-288-3035, option 1 to report:

- Unauthorized access or transactions on your Concourse accounts
- Lost or stolen online access information
- Suspicious emails or websites referencing Concourse

Risks of Using Electronic Communications

Technology has made it easy for hackers to cast a very broad net in their quest to obtain confidential information instantaneously and cheaply. With the press of a button, a hacker can launch 100,000 emails to as many potential “marks” containing malicious email or text, all designed to provide access to the information on your computer, mobile device, and related online accounts. This disclosure provides basic steps you can take to enhance your cyber security.

Email Communications: Be Alert to Phishing Attempts

Beware of attempts to "phish" your information. These are often in the form of urgent-sounding emails where you might be encouraged to click on a link in order to update personal information. Even clicking on the link could potentially take you to a malicious website where malware could infect your computer. We strongly recommend that you not click on suspicious links. Instead, navigate directly to a known web address.

Do not open emails from senders you do not recognize. Never open attachments or click on embedded links unless you are sure of their authenticity. This is true even if the email appears to come from someone you know. Remember, it is very common for hackers to learn the email addresses of individuals in your network and send emails that appear to come from similar addresses (e.g., John.Smith@concoursefinancialBD.com).

Website Security

Before entering any information on a website, check the URL to see if it begins with “https”. The safest method to access a website is by entering the URL into your browser window or accessing it via your saved favorites. Avoid clicking links from emails or pop-ups, as it could direct you to a malicious site.

Cybersecurity Away from Home

Avoid using public computers to access accounts or sensitive information. If you have to use a shared device, take steps to log out of online accounts before you use the device. Otherwise, after you use the device, immediately change the passwords to any site you accessed on the shared device.

Avoid public Wi-Fi hotspots, like those at airports, coffee shops, stores, hotels, etc. Stick to the cellular network or use a VPN service to encrypt your data.

Avoid publicly available charging cords or USB ports----plug your cord directly into the power source. These devices can be used to deliver malware onto your device.

Set your screen lockout time as short as possible (e.g., one minute). This will help ensure no one can use your device if you lose it or leave it unattended. Also, be sure to use your Find My iPhone or equivalent technology. This helps you locate a lost device and, if necessary, erase your device remotely if necessary.

Cybersecurity at Home

Technology changes quickly. Keep your computer's antivirus and firewall software current. Ensure your computers are encrypted. Auto-install essential operating system updates. Lock your computer and mobile devices when not in use.

Use secure Wi-Fi and change your router's default password. Consider using a mesh network with enhanced security to protect your devices.

If your finances allow it, consider having one standalone dedicated device just for your banking and financial activities, and nothing else (no web browsing, email, etc.).

Create Strong Passwords and PINs

Hackers can crack a six-letter password in minutes. By adding uppercase letters, symbols, and numbers, the time it would take to crack your passcode increases exponentially. Avoid the most common passwords, like "123456" or "password." Also avoid using your children's names, your pet's name, the last four digits of your SSN, or any other item of information that may be readily accessible by others.

Memorize your passwords and PINs, and not write them down. Do not share your passwords and PINs with anyone, even if someone asks. Note: Your financial institutions will not ask you for this information. Finally, change your passwords and PINs regularly, especially if you suspect that someone may have knowledge of them. Do not reuse passwords or use the same password for multiple sites. Password managers help create secure passwords and store them in an encrypted state.

Use Multifactor Authentication (MFA)

MFA absolutely enhances the security of your online experience. If your financial institution allows, you should use more than one method of authentication, such as a password and a text code or a one-time password and challenge question. Some websites offer an authorization code, which is a one-time number sent via email or text when you log in. Use biometric safeguards (fingerprint, facial recognition, etc.,) if they are available.