Protecting Investors from Cybercrime

Safeguards to Help Minimize the Risk of Theft or Loss of Your Personal Information and Data

What Modera Is Doing to Protect Your Information

Recent news regarding data breaches of retailers, financial institutions, those in the financial services industry and even some governmental offices emphasizes the need for both offensive and defensive strategies to defend electronic data. The stakes are high for all of us as hackers and thieves try to obtain your personal information. While scams are constantly evolving and there can be no guarantee of ironclad defenses, the following measures are designed to help minimize possible exposure to cybercrime.

Federal and state privacy laws require investment advisory firms to adopt policies and procedures to protect your privacy. Modera commits significant financial and human capital resources on both the compliance and technology fronts to seek to maintain the privacy and protection of your data. Working with outside regulatory counsel, we have organized these policies and procedures as part of our compliance documents, including our privacy policy, red flags policy and Information Security Plan. The firm also imposes on all offices the duty to adhere to the Commonwealth of Massachusetts' privacy laws, generally considered the toughest in the nation.

MODERA'S CYBERSECURITY STRATEGY

Assess

- Regular scans and penetration testing to evaluate network integrity
- Regular staff assessments of security protocols
- Dedicated IT Manager and IT Consulting Firm to monitor emerging threats and respond as appropriate

Implement

- Use of firewalls to restrict information flow and hide presence of network from outside world
- Mandatory cybersecurity training, including social engineering education, for all staff
- Enterprise-level anti-virus protection
- Secure network accessed only by unique ID, password and dual-factor authentication
- Network access via secure VPN

Maintain

- Persistent monitoring
- Current software security updates, and operating system patches
- Encryption and secure communication
- Servers housed in the cloud and full data backups housed in a separate data center
- Inventories kept of network accessing devices

What Your Custodians and Tamarac Are Doing to Protect Your Accounts

Your custodian restricts who can access your information. Our three recommended custodians keep behind-the-scenes security measures and practices private to make it more difficult for fraudsters to understand the tools and techniques they apply.

YOUR CUSTODIAN USES VARIOUS SECURITY MEASURES, INCLUDING THE FOLLOWING:

Schwab

- Data encryption on data in transit.
- Extended Validation Certification: this is the green bar in front of the web address that confirms you are truly on Schwab's website.
- "https://" and padlock icon in the address bar will additionally confirm you are on the secure site.

Fidelity

- Dual-factor authentication through Symantec's Validation and ID Protection (VIP). Application generates a random code to authenticate your access as well as your user name and password.
- 128-bit two-way data encryption for all communications with website.

TD Ameritrade

- 128-bit encryption on data communications between your computer and its site.
- 3rd party specialist is retained to monitor for potential identify theft.
- Anomaly and intrusion detection software is used.

Modera Client Hub *(Tamarac AdvisorView)*:

- 128-bit SSL encryption – the same protection banks and financial institutions use – to help keep your information protected from unauthorized access. Your information is backed up to an SSAE-16 and SAS70 Type II compliant data center. Tamarac is SOC 1 Type II/ SSAE-16 certified.

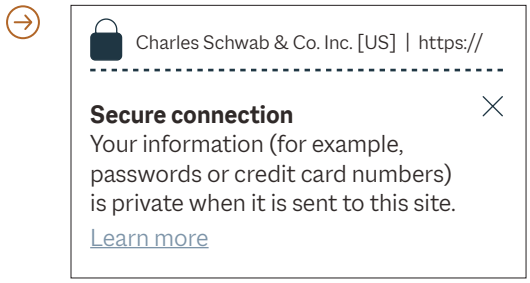
Tamarac and our recommended custodians offer you the option to use dual factor authentication when logging in to access your account information. To help protect your account information on these platforms we strongly recommend that you use dual factor authentication to help increase security.

You should check your account statements and trade confirmations regularly. Include checking the spelling of your name, address and account numbers for any discrepancies.

What You Can Do To Help Protect Yourself

GENERAL SECURITY MEASURES

- Update/Patch: Keep your software up to date through applying any available patches and updating to the most current version.
- Install anti-virus and anti-spyware software on all platforms (Windows, Apple and mobile devices).
- Be vigilant online. Secure websites will have one or all of the following:
  - Green bar and/or padlock
  - https:// URL address



- Each secure site comes with a digital certificate, establishing its legitimacy. To view the certificate, double click on the lock or key.
- If you get a pop-up message indicating a problem with a site's Security Certificate, do not proceed.
- Empty your browser cache so that stored information can't be hacked.
- When you are finished accessing your account at the custodian or Tamarac, always log off and close your browser. Use a pop-up blocker to reduce potentially harmful threats.
- 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 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.
- Don't reply to emails asking for personal information and don't click on links sent by parties you don't know. Instead, right click on a link and select properties. If the @ symbol is under the URL address, it is likely fraudulent. If necessary, contact the sender in question by telephone. Turn off the "preview pane," as this allows some viruses to be executed even if you never actually open the email.
- Place credit freezes on your accounts with the credit bureaus. Contact your wealth management team for specific information on how to do so.

MOBILE DEVICE SECURITY PRECAUTIONS

- Password protect your devices and enable auto-lock.
- Use strong, hard-to-guess passwords – 8 characters or more if possible.
- Do not share your password with anyone and, if compromised, change it immediately.
- Only download apps from the Google Play Store or Apple's App Store.
- Do not use public Wi-Fi to access sensitive data (such as your banking app).
- Allow for remote wipe of your device if it is lost or stolen.
- Control third-party software: when installing a new app to your device, check to see what it's accessing on your device. For example, many retail apps require access to your camera, contacts and location. Consider whether you are comfortable with this level of access.
- Review third-party software information sharing policies: the reason most apps want access to all your data is to share it with other parties.
- Set your phone to auto-wipe after a set number of incorrect password entries.
- Routinely backup your mobile device.
- Be wary of phone vishing which is phishing for information over the phone.

If you doubt the security of an open wireless network, don't use it. Shut off wireless connectivity or remove the wireless network card. If you leave your computer unattended, disable the wireless mode to prohibit any unauthorized wireless network access.

If you use a wireless connection, select one that is rated WPA2 and turn off file sharing. Use of a wireless network presents several security concerns. Wired Equivalent Privacy (WEP) is the standard encryption that wireless devices use. If your wireless network supports WPA or WPA2 you should select that option rather than WEP. Because this encryption can be breached, make sure you take these steps:

1 **Change the administrator password.**

After you remove your Wi-Fi router out of the box, you'll be prompted to log into it through a web page using a specified username and password. That username and password is identical for all models of your router-an open invitation to hackers because these common passwords are published by numerous sites. See above for information on creating secure passwords.

2 **Change the default Service Set Identifier (SSID).**

The manufacturer of your router sets all its routers to the same SSID, for example "default" or "Linksys." While the SSID doesn't allow hackers to get in, a default setting often signals them that the owner hasn't taken the proper security precautions. You can change this setting in the setup page of your router.

3 **Only access personal information through Web sites that use Secure Sockets Layers (SSL).**

4 **Disable file and printer sharing capabilities when you're connected to a public wireless network.**

Additional information to help you:

- **SEC Publication:** "Online Brokerage Accounts: What You Can Do to Safeguard Your Money and Your Personal Information" (*http://www.sec.gov/investor/pubs/ onlinebrokerage.htm*)
- **SEC Investor Alert:** "Identity Theft, Data Breaches and Your Investment Accounts" (*http://www.sec.gov/oiea/ investor-alerts-bulletins/ia_databreaches.html*)
- **FINRA Investor Alert:** "Protect Your Online Brokerage Account: Safety Should Come First When Logging In and Out" (*http://www.finra.org/Investors/ProtectYourself/ InvestorAlerts/TradingSecurities/p014769*)
- **FTC OnGuardOnline.gov webpage:** "Tips for Using Public Wi-Fi Networks" (*http://www.onguardonline.gov/articles/0014-tips-usingpublic-wi-fi-networks*)

What We Can Do Working Together to Help Protect You

Knowing your spending patterns and your third-party relationships can help us identify suspicious activity or requests.

Our Asset Transfer Verification Policy requires a member of your wealth management team to speak with you in person or by telephone, at a telephone number on record with us, to verify a new request to transfer your assets.

We will not:

- verify a requested asset transfer by sending an email message to you;
- send your personal information via email (unless you choose not to use the Client Hub vault and the email is password protected); or accept an incoming call from a number unfamiliar to us offering confirmation of a requested asset transfer.

To help protect yourself:

- use the dual factor authentication tools that your Client Hub and your custodian offer;
- provide your personal information to us only via a secure vault in your Client Hub;
- if you chose not to use the Client Hub vault, **never** send personally identifying information like account or social security numbers in the text of, or as an unprotected attachment to, an email.

What Should You Do If You Suspect Fraud?

IF YOU SUSPECT FRAUD OR IDENTITY THEFT, THE FASTER YOU ACT THE BETTER. HERE IS WHAT YOU SHOULD DO RIGHT AWAY.

Step 1:

If the event occurs during our regular business hours, contact us.
Otherwise, contact your custodian first. Then contact us.

- **Schwab:** Call 800-435-4000. If you're abroad, call +1-602-355-7300
- **Fidelity:** Call 800-544-6666
- **TD Ameritrade:** Call 800-400-6288

Step 2:

If unauthorized activity is confirmed, let one of the credit bureaus know (the other two will be notified automatically) and place a credit freeze on your accounts.

- **Equifax:** Call 800-525-6285, or visit *www.equifax.com*, or write P.O. Box 740250, Atlanta, GA 30374.
- **Experian:** Call 888-397-3742, or visit *www.experian.com*, or write P.O. Box 9556, Allen, TX 75013.
- **TransUnion:** Call 800-680-7289, or visit *www.transunion.com*, or write P.O. Box 6790, Fullerton, CA 92634.

Step 3:

Notify the appropriate government agency.

- Visit the *FTC's Identity Theft Site* to learn more.
- Forward suspicious emails to: *nophishing@cbbb.bbb.org*.

Contact us for more information:

Terry Days
Chief Compliance Officer at Modera Wealth Management
617-247-0518
terryd@moderawealth.com

Modera Wealth Management, LLC ("Modera") is an SEC registered investment adviser. SEC registration does not imply any level of skill or training. Modera may only transact business in those states in which it is notice filed or qualifies for an exemption or exclusion from notice filing requirements. For information pertaining to Modera's registration status, its fees and services please contact Modera or refer to the Investment Adviser Public Disclosure Web site (adviserinfo.sec.gov) for a copy of our Disclosure Brochure which appears as Part 2A of Form ADV. Please read the Disclosure Brochure carefully before you invest or send money. Nothing contained herein should be interpreted as legal, tax or accounting advice nor should it be construed as personalized investment advice.