Modera's Cybersecurity Policy Overview

Our firm's security policy helps minimize the risk of theft or loss of your personal information and data.

What Modera is doing to protect your information

It seems the news is constantly reporting on data breaches. Sadly, nobody is immune from this threat.

At Modera, we recognize the need for both offensive and defensive strategies to protect 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, this guide details the measures Modera Wealth Management and our recommended custodians take to help ensure your financial information is safe from cybercrime. In addition, we offer some helpful tips you can follow to minimize possible exposure to cybercrime and to help protect you and your accounts from becoming a victim.

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 help 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 Information Security Policy, Red Flag Policy, Asset Transfer Verification Policy and Privacy Policy. It is a requirement that all offices 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 staff and IT Consulting Firm to monitor emerging threats and respond as appropriate

Implement

- Use of firewalls to filter traffic, restrict information flow and hide presence of local networks from outside world
- Mandatory quarterly cybersecurity training, including social engineering education, for all staff
- Modern enterprise-grade endpoint protection for all servers and workstations
- Secure network utilizing multifactor authentication
- Network access via secure VPN

Maintain

- 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 maintained of all IT assets

A key component of assessing and implementing our cybersecurity strategy is staying vigilant against the threat that "threat actors" impose on your financial security. While investment advisers are not typically considered financial institutions or creditors, Modera procedures incorporate industry guidelines designed to identify, detect and respond to relevant types of identity theft red flags with respect to financial accounts.

Examples of possible red flags are:

- Mail sent to the client is returned repeatedly as undeliverable.
- Modera is notified that the client is not receiving paper account statements from the custodian or reports from the firm.
- A "client" uses an account or makes requests that are not consistent with established patterns of activity on the account or the known personality, history or general wishes of the client.
- Shortly following the notice of a change of address, Modera receives a request for credentials to access the account or a substantial distribution of assets to the new address.

We take the time to get to know our clients and their lives. Knowing your usual transactions and spending patterns as well as your third-party relationships can help us identify suspicious activities or requests should they occur.

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.

If an identity theft threat or any nefarious attempt is detected on a financial account managed by and accessible to Modera, we will respond and escalate appropriately.

What your custodians are doing to protect your accounts

Both of our recommended custodians, Schwab and Fidelity, are well-versed in cybersecurity threats, trends and preventative tactics. Here are a few of their high-level security measures:

SCHWAB

- **Multi-layered technology:** Their sites feature encryption and risk-based security technology. These controls, combined with automated alerts, an identity verification process and rigorous monitoring, help defend against unauthorized account access.
- **Highly trained specialists:** Employees who handle sensitive information are trained in privacy and security.
- **Secure process and procedures:** Whether you call, visit a branch or go online, your identity will be verified before any sensitive information is discussed.
- Learn more about their security policy: *schwab.com/schwabsafe*

FIDELITY

- **Multi-factor authentication:** If elected, for extra protection during logins and sensitive transactions, you will get a push notification or security code to verify it's you.
- **Money transfer lockdown:** They will block electronic money movement out of your accounts, protecting your balances from unauthorized transfers.
- **Security text alerts:** If elected, you will get instant security alerts on your mobile number when certain transactions or profile updates are made to your account.
- **Fidelity voice biometrics:** They use voice biometric technology in two ways to verify clients by voiceprint over the phone or through any microphone-enabled digital device.
- Learn more about their security policy: *fidelity.com/security*

What you can do to help protect yourself

You are the first and best defense against becoming a victim of cybercrime. We strongly encourage our clients to:

1. **Review accounts and statements:** Check your account statements and trade confirmations regularly for mistakes or unauthorized activity. Check the spelling of your name, your address, and account numbers for any discrepancies. Set up security alerts to know immediately when activity occurs in your account(s).

2. **Use dual factor authentication:** Our recommended custodians as well as our client hub offer the use of dual factor authentication. The added step in verifying your identity is another layer of security that can prevent a criminal from accessing your accounts.

3. **Use strong passwords:** Use a unique password across all your accounts and applications and change them frequently. Never give anyone your password or leave them unprotected, such as on a piece of paper or in a non-secure app. Consider using a password manager app to store all your passwords securely.

4. **Keep sensitive information private:** Do not send any personally identifying information such as social security or passwords in emails. Never share account numbers or email sensitive documents, such as tax returns or account statements as attachments. We will never ask you to do this and will always encourage the use of our secure client hub.

5. **Be careful where you click:** The best way to avoid malicious links is to not click on them. Do not reply to or download documents from an email or text from an unknown source or pop-up window. Doing so can expose your device to malware and provide access to your personal information.

6. **Be vigilant online:** Do not visit non-secure or unknown websites. Look for the key or pad lock symbol or https:// preceding the URL address. Make certain to log out of any application you are using when you are finished and then close the web page and browser.

7. **Keep devices secure:** Install security software that includes antivirus, anti-spam and spyware. Configure your devices to receive automatic updates to ensure they are running on the latest software and security available. Stay up to date with all your device system upgrades and versions. Do not give anyone access to your devices and empty your browser cache so that stored information can't be hacked.

8. **Use secure Wi-Fi:** Only use a trusted, encrypted network, especially when accessing your financial accounts. Public hot spots such as those found in hotels and airports are far less secure and provide easy access for hackers to intercept your information.

9. **Freeze your credit:** It's a good idea to put a freeze on your credit with the credit bureaus. Doing so restricts access to your credit report and can protect you from fraudulent activity in the event your identity is stolen. Contact the credit bureaus directly (see next section for contact information) or your wealth management team for specific information on how to do so.

10. **Monitor your credit reports for suspicious or unauthorized activity:** Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit *www.annualcreditreport.com* or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Contact the Federal Trade Commission and your state Attorney General to learn more about identity theft, fraud alerts, credit freezes, and other steps you can take to protect yourself. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, *identitytheft.gov*, 1-877-ID-THEFT.

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:

Change your username and passwords immediately. During our regular business hours, contact us. If after business hours, contact your custodian first, then contact us.

- **Schwab:** Call 800-435-4000.
  If abroad, reference: *schwab.com/contact-us/international-toll-free-numbers*
- **Fidelity:** Call 800-544-6666.
  If abroad, reference: *fidelity.com/customer-service/phone-numbers/international*

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 if you haven't done so already.

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

STEP 3:

Report incidents of suspected or actual identity theft or fraud to law enforcement, the Federal Trade Commission, and your state Attorney General.

For more information on these and other cybersecurity and safety topics, please visit our website *https://moderawealth.com/category/cyber-security/*.