HOW WE PROTECT YOUR PERSONAL AND FINANCIAL INFORMATION

As your financial advisor, safeguarding the personal and financial information you have entrusted to me and my team is of paramount importance. Of the many reasons I choose to partner with Commonwealth Financial Network® to help me manage your financial life, there is none more important than the comprehensive level of information security the firm provides.

I hope the information below answers the key questions you have regarding your data and how it's handled. Of course, if you would like to discuss anything, please don't hesitate to contact me.

Q: Who has access to my data and where is it stored?

A: All of the financial and personal information that is accessible to me and others in my office is managed on computers connected to Commonwealth's proprietary, secure network. Each person in my office with access to your data has a unique secure login, and we are required to change our passwords every 90 days. Your data is kept at multiple redundant data centers managed by Commonwealth, which implements strong security controls to protect the confidentiality, integrity, and availability of your information.

Q: What safeguards does Commonwealth have in place to protect my personal information and assets?

A: Commonwealth has implemented policies and procedures, including a written information security program (WISP) designed to safeguard our clients' personal information and assets. Commonwealth's WISP complies with all applicable privacy and data security laws, and Commonwealth regularly reviews it to address and mitigate new risks as they develop.

Q: Does Commonwealth monitor my personal information to determine whether it has been stolen or misused?

A: Commonwealth uses sophisticated programs that monitor the transmission of sensitive client information. In addition, it has policies and procedures in place to verify customer inquiries and transaction requests.

Q: How does Commonwealth handle an account intrusion or other malicious cyber event? For example, would I be notified if personal information or assets were compromised—and how would I receive this notification?

A: Commonwealth has an Information Security team that investigates all incidents of privacy intrusion. The team determines the scope of the incident and which clients may have been affected. Commonwealth will notify clients if there is a material risk that an unauthorized party has accessed any client information and whenever notification is required by law.

Q: Will Commonwealth reimburse me if my assets are compromised by a cyber attack?

A: In general, once it has been determined that an unauthorized transaction has occurred, Commonwealth will promptly reimburse clients for losses.

Commonwealth has obtained a privacy liability and network risk insurance policy to cover the costs associated with investigating and responding to breaches of client information. This policy covers, among other things, the costs associated with determining the scope of a breach, notifying clients, and offering credit-monitoring services to affected clients.

Q: Has Commonwealth addressed the cybersecurity threats and vulnerabilities that may impact its business?

A: Yes, Commonwealth conducts ongoing risk assessments to determine cybersecurity threats and vulnerabilities that may impact its business. The firm performs cybersecurity risk assessments using third-party security companies, internal technology professionals, and internal audit staff. In addition, Commonwealth employees and advisors are trained to proactively identify and report potential risks to the Information Security team.

Q: Does Commonwealth have written policies, procedures, or training programs in place pertaining to safeguarding client information?

A: Yes, as noted previously, Commonwealth has a WISP in place, as well as various policies and procedures designed to protect client information. Its Information Security program deploys a defense-in-depth strategy, in which multiple layers of security are used. Safeguards include key-access door controls, network access and authentication controls, and data-loss-prevention software that monitors sensitive information into and out of the network.

Members of Commonwealth's Information Security and Technology departments regularly review and perform internal audits of the firm's policies and procedures to ensure restricted access to clients' sensitive information and also to ensure that Commonwealth is compliant with all federal and state regulations.

Q: Does Commonwealth maintain insurance coverage for cybersecurity?

A: Yes, Commonwealth maintains a $10 million privacy liability and network risk insurance policy to cover the costs associated with investigating and responding to breaches of client information. This policy covers, among other things, the costs associated with determining the scope of a breach, notifying clients, and offering credit-monitoring services to affected clients.

Q: Has Commonwealth engaged an outside consultant to provide cybersecurity services?

A: Yes, Commonwealth has hired several technology firms that specialize in information security to perform risk and vulnerability assessments and penetration tests. In addition, its Information Security team employs an experienced and credentialed staff of technology and privacy professionals.

Q: Does Commonwealth have confidentiality agreements with third-party service providers that have access to your information technology systems?

A: Yes, all agreements with third-party service providers who may access sensitive client information include confidentiality language that describes each party's obligations with regard to how they handle sensitive information. In addition, Commonwealth performs initial and ongoing due diligence on third-party service providers.

Q: Does Commonwealth use safeguards such as encryption, antivirus, and antimalware programs?

A: Yes, Commonwealth employs advanced encryption, state-of-the-art firewall technologies, and advanced antivirus and antimalware programs. Data is encrypted using advanced encryption algorithms.

Q: Do you, as my advisor, contact clients via e-mail or other electronic messaging? If so, do you use secure e-mail, as well as procedures for authenticating client instructions received via e-mail or electronic messaging, to work against the possibility of client impersonation?

A: Commonwealth's policy requires all electronic communications with sensitive information to be sent via encrypted e-mail. Commonwealth provides us with a secure e-mail system for use when e-mailing sensitive information. In addition, Commonwealth policy requires us to verify all third-party distribution requests directly with our clients via telephone.

WALTHAM OFFICE
29 SAWYER ROAD
WALTHAM, MA 02453-3483
TOLL-FREE: 800.237.0081
PHONE: 781.736.0700
MAIN FAX: 781.736.0793

SAN DIEGO OFFICE
110 WEST A STREET, SUITE 1800
SAN DIEGO, CA 92101-3706
TOLL-FREE: 877.347.1982
PHONE: 619.471.9700
MAIN FAX: 619.471.9701

COMMONWEALTH.COM
COMMONWEALTH FINANCIAL NETWORK®
MEMBER FINRA/SIPC

TECHN-3080-28197_10/16