FAQs: How We Protect Your Personal and Financial Information

As your financial advisor, safeguarding the personal and financial information you have entrusted to Commonwealth Financial Network,® the firm we partner with to better serve you, and to my team is of paramount importance.

Of the many reasons I choose to partner with Commonwealth to help me manage your financial life, there is none more important than the comprehensive level of security the firm provides. The following frequently asked questions highlight the various ways we protect your personal and financial information.

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

All financial and personal information 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 passwords every 180 days. Password policies align with industry best practices and require us to create longer passwords.

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?

Commonwealth has implemented "Data Loss Prevention," along with other cybersecurity tools, and offers 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.

In addition, Commonwealth uses data classification to ensure that data is protected based on its level of sensitivity, access controls to limit who has access to what data based on job roles, and encryption to secure information in transit (data moving between devices or networks) and at rest (data that is not moving between devices or networks).

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

Commonwealth uses sophisticated programs in a process called "Data Loss Prevention" that monitors the transmission of sensitive client information. Any connected networks and systems are constantly monitored for malicious actors to initiate an efficient and effective response in the event of an incident. In addition, we have policies and procedures in place to verify customer inquiries and transaction requests.

Derrell Crimm, CFP®
AC Financial Partners
1800 International Park Drive | Suite 10 | Birmingham, AL 35243
205.235.3500 | 205.235.5170 fax | www.acfinancialpartners.com | derrell.crimm@acfinancialpartners.com

Q How does Commonwealth handle an account intrusion or other malicious cybersecurity event(s)? Would I be notified if personal information or assets were compromised, and how would I receive this notification?

Commonwealth has a Privacy team and an Information Security team that investigates all incidents of privacy intrusion. The teams determine 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 cyberattack?

In general, once it has been determined that an unauthorized transaction has occurred, Commonwealth will promptly reimburse clients for losses. Commonwealth has obtained a Cyber Liability 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 cybersecurity threats and vulnerabilities that may impact its business?

Yes Commonwealth conducts ongoing risk assessments and vulnerability scanning 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, internal security tools, 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?

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, encryption, network and system monitoring, and data classification 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 assessments of the firm's policies and procedures to ensure restricted access to clients' sensitive information and to ensure that Commonwealth is compliant with all federal and state regulations. In addition, simulated phishing assessments and trainings are performed on a regular basis to raise awareness of current cyberthreats for Commonwealth employees and advisors.

Q Does Commonwealth maintain insurance coverage for cybersecurity?

Yes. Commonwealth maintains a $15 million Cyber Liability 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?

Yes. Commonwealth has hired several technology firms that specialize in information security to perform risk and vulnerability assessments and penetration tests to understand key threats, vulnerabilities, and potential gaps in capability, to continually improve its information security program to combat current and emerging threats. 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?

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

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

Commonwealth provides us with a secure email system for use when emailing personal information; it automatically encrypts email when specific fields/attributes are identified in the email, such as social security numbers and account numbers. Commonwealth's Information Systems and Office Security Policy requires all electronic communications with such personal information to be sent via encrypted email through the secure email system.

Manual encryption is also in place to encrypt all other personal information such as passport numbers and medical-related information for added layers of protection. Our email security system continuously scans inbound and outbound email for threats and malicious content, as well as automatically encrypting personal information when it is detected.

For more information on the collection, use, and storage of your information with Commonwealth, please refer to Commonwealth's Privacy Notice. In addition, Commonwealth's Compliance Manual requires us to verify all third-party distribution requests directly with our clients via telephone.

I hope this information answers key questions you may 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.