

[October XX, 2024]

[Client Name]
[Street Address]
[City, State, Zip Code]

Dear [Client Name],

Sophia Wealth Strategies is writing to notify you about a recent data security incident that may have involved your personal information. We take the privacy and security of your information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter is intended to provide information about our response to the incident and to provide you with resources to help protect your information from possible misuse.

The data access may have included personal information, such as your full name, social security number, account number, date of birth, and email address. The investigation did not uncover any evidence that unauthorized use of information has occurred; however, it's recommended that you monitor your accounts for any suspicious activity.

Although we are unaware of any misuse of your information, Commonwealth has arranged for Kroll to provide complimentary credit monitoring to you for 18 months as an added precaution. To take advantage of this offer or to add restrictions to your account as an extra safeguard, please contact me by phone or email. Please also review the attachment to this letter to learn more about how to protect your personal information.

We deeply regret that this incident occurred. If you have any questions, please contact us at 413-341-6101 and we will address your concerns.

Sincerely,

Melody A. Foti, CFP®

Steps to Further Protect Your Information

1) Review your account statements and notify law enforcement of suspicious activity

If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 877.438.4338. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

2) Obtain a copy of your credit report

Under federal law, you are entitled to one free credit report every 12 months from each of the three major credit reporting agencies below. Call 877.322.8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Equifax
800.349.9960
www.equifax.com

Experian
888.397.3742
www.experian.com

TransUnion
888.909.8872
www.transunion.com

3) Place a fraud alert on your credit report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

4) Put a security freeze on your credit file

In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name that is issued to you when you initiate the freeze. A security freeze is designed to prevent fraudsters from accessing your credit report without your consent. Using a security freeze may interfere with or delay your ability to obtain credit, however. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, social security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.

5) Access additional free resources on identity theft

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit www.ftc.gov/idtheft or call 877.438.4338.