

Stephen P. McCarthy
Certified Public Accountant

RE: Notice of Data Breach

October 18, 2024

Office of Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Dear Office of Attorney General,

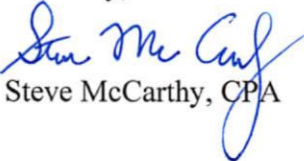
On May 8, 2024, we experienced a network disruption that limited our ability to access certain files and systems on our network. We immediately began an investigation with the assistance of third-party specialists (Cyberscout) to determine the full nature and scope of the incident. The investigation determined we were the victim of a ransomware attack.

1 Maryland Resident was impacted by this breach. We will notify them with the attached letter.

Information that may have been breached: name, date of birth, telephone number(s), address, social security number, W-2 information, and 1099 information.

Steps Taken to Restore Integrity of System: In response to this incident, we implemented additional security measures to protect our network further and reduce the risk of a similar incident occurring in the future. In addition, all of our data is now stored in the cloud.

Sincerely,


Steve McCarthy, CPA

Stephen P. McCarthy, CPA
c/o Cyberscout
[Cyberscout Address]

[Date]

[Recipient's Name]
[Address]
[City, State, Zip]

[Use for Maryland residents]

NOTICE OF DATA BREACH

Dear [Recipient's Name],

Please read this letter in its entirety.

We are writing to provide you with a formal notification regarding a data incident that occurred at Stephen P. McCarthy, CPA, in which your personal information may have been accessed by an unauthorized user. This letter serves to provide additional information concerning the incident, what is being done to correct it, and what you can do to further protect your information.

What Happened?

On May 8, 2024, we experienced a network disruption that limited our ability to access certain files and systems on our network. We immediately began an investigation with the assistance of third-party specialists to determine the full nature and scope of this incident. The investigation determined that we were the victim of a ransomware attack. Unfortunately, these types of incidents are becoming increasingly common and organizations with some of the most sophisticated IT infrastructure available continue to be affected.

We have no information that your sensitive data has been misused in any manner by the threat actor, or that your tax returns have been impacted in any way. That said, we are taking appropriate precautionary measures to protect your financial security and to help alleviate concerns you may have. If we become aware of any suspicious activity in connection with your tax returns, we will notify you immediately. Conversely, if you receive any notifications from the IRS concerning suspicious activity on your account, please notify our office right away.

What Information Was Involved?

For Individuals: While our investigation has not revealed the precise information which may have been accessed by the threat actor, the information could have included your name, gender, date of birth, telephone number(s), address, social security number, employment (W-2) information, 1099 information, as well as direct deposit bank account information, including

account number and routing information, and/or other information you may have also provided to us.

For Entities: While our investigation has not revealed the precise information which may have been accessed by the threat actor, the information could have included your company name, Federal Employer Identification Number, address, telephone number, employee and/or 1099-recipient information, partner, shareholder/officer or beneficiary names, addresses, social security numbers, and/or other information you may have also provided to us.

What We Are Doing.

In response to this incident, we implemented additional security measures to further protect our network and reduce the risk of a similar incident occurring in the future.

Further, we are working with the appropriate agencies on your behalf. The FBI and Secret Service have been notified of this incident. This notification to you was not delayed as a result of law enforcement investigation.

At this time, we have no evidence of attempted or actual misuse of any information as a result of this incident. However, in response to the incident, we are providing you with access to **Triple Bureau Credit Monitoring** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

We are taking this matter very seriously and are committed to helping those people who may have been impacted by this unfortunate situation.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do.

If you have not done so already, you should do the following:

If you choose not to use the offer of Credit Monitoring by Cyberscourt and choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.)
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- You may also want to consider contacting these three credit agencies at the phone numbers above to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report, making it less likely that an identify thief can open new accounts in your name. There is no cost to place and lift a freeze. (See below for more information.)
- Be sure to promptly report any suspicious activity to Stephen P. McCarthy, CPA.

- We strongly suggest you contact the IRS about getting an Identity Protection PIN to use with your Social Security Number for heightened security. You can do this by going to <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>. The initial process to register for the PIN will only take about 10-15 minutes.
- Freeze your credit at the three major credit agencies - TransUnion www.transunion.com, Equifax www.equifax.com, and Experian www.experian.com. This process is surprisingly simple and only takes 20 to 30 minutes to complete.
- Consider notifying your bank(s) to see if they have any suggestions to enhance the security on your accounts.
- We strongly recommend you be vigilant in reviewing your bank accounts and other financial account statements, as well as monitoring your Credit Monitoring or free credit reports. You are entitled, pursuant to the federal Fair Credit Reporting Act, to a free credit report from each nationwide credit bureau and from nationwide specialty consumer reporting agencies once every 12 months. You are also entitled to dispute incomplete or inaccurate information. You may obtain your free credit report from each of the three major credit reporting agencies at www.annualcreditreport.com.
- If you suspect identity theft, report it to law enforcement, including the Federal Trade Commission at <https://www.identitytheft.gov/#/> and your State Attorney General's Office at <https://www.naag.org/find-my-ag/>.
- You can obtain more information from the above three credit bureaus, Federal Trade Commission, and your State Attorney General's Office about identity theft, fraud alerts, security freezes, and the protection of your sensitive information. The Federal Trade Commission can be contacted as follows:

- **Federal Trade Commission**
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-382-4357
<https://www.consumer.ftc.gov/>

The Maryland Attorney General can be contacted as follows:

- **Maryland Attorney General**
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
<https://www.marylandattorneygeneral.gov/#>

For More Information.

We are committed to helping those people who may have been impacted by this unfortunate situation. Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. Should you have additional questions or concerns regarding this matter, please do not hesitate to contact Cyberscout's dedicated call center at ###-###-#### Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Time (excluding U.S. national holidays).

If you wish to reach Stephen P. McCarthy, CPA, you can email us at Ryan@mamportfolios.com or Steve@mamportfolios.com, or call us at 650-610-9540.

Sincerely,

Steve McCarthy