2024-423

Arsenault and Cline CPA's Inc
c/o Cyberscout
1 Keystone Ave, Unit 700
Cherry Hill, NJ 08003
DB-08458

[redacted]

March 1, 2024

IMPORTANT INFORMATION – PLEASE REVIEW CAREFULLY

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to Arsenault and Cline CPA's Inc. We're writing with important information regarding a data security incident that involved some of your personal information. We want to notify you of the incident and explain the services we are providing to you.

On or about July 10, 2023, Arsenault and Cline CPA's Inc. experienced a security incident. Upon learning of this issue, we took steps to ensure the security of our systems and we commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals experienced in handling these types of situations to assist us in determining the full extent of the incident and scope of any data impacted.

Our comprehensive investigation and review recently concluded on February 6, 2024 and determined that the security incident involved some of your information, including your first and last name and [redacted]

We wanted to make you aware of the incident and suggest steps that you should take to protect yourself. This letter provides precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. If your bank account information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis and report any unusual activity to the payment card brand or the institution that issued the statement, as well as law enforcement.

Finally, we are providing you with access to Single 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 your credit file. 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to [redacted] 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.

We regret any concern this caused you, and we sincerely appreciate your patience as we continue our efforts to resolve this matter. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any additional questions, please contact the external, dedicated call center we set up at [redacted] between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. The call center is available for 90 days from the date of this letter.

Sincerely,

Arsenault and Cline CPA's Inc
150A Andover St #7a
Danvers, MA 01923

– OTHER IMPORTANT INFORMATION –

1. **Placing a Fraud Alert.**

You can place an initial one (1) year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888)-298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** 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 company.

4. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington,

DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Reporting Identity Fraud to the IRS.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), it is recommended that you do the following:

- **File an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf)**
  - This form can be submitted online (https://apps.irs.gov/app/digital-mailroom/dmaf/f14039/) or it ca be mailed or faxed to the IRS: Department of the Treasury, Internal Revenue Service, Fresno, CA 93888-0025; 855-807-5720
  - ***Please note that this form should be used only if your Social Security number has been compromised and the IRS has informed you that you may be a victim of tax-related identity fraud or your e-file return was rejected as a duplicate.**
  - You may choose to opt-in to the IRS Identity Protection (IP) PIN Program. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. To opt-in, you should use the online "Get an IP PIN" tool (which can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin). If you don't already have an account on IRS.gov, you must register to validate your identity. An IP PIN is valid for one calendar year. You must obtain a new IP PIN each year. The IP PIN tool is generally unavailable mid-November through mid-January each year.
  - If you are filing Form 14039, you should also check with your local state tax agency to see if there are any additional steps to take at the state level for reporting tax-related identity theft;
  - A complete listing of each state tax agency's website can be found at: https://www.taxadmin.org/state-tax-agencies.
  - Review guidance from the IRS about tax-related identity theft at: https://www.irs.gov/uac/taxpayer-guide-to-identity-theft (Taxpayer Guide to Identity Theft) and https://www.irs.gov/pub/irs-pdf/p5027.pdf (IRS Publication 5027, Identity Theft Information for Taxpayers); and/or
  - Call or visit your local law enforcement agency and file a police report.

Keep in mind that if you have an open identity theft case that is being worked on by the IRS, you need to continue to file your tax returns while the investigation is ongoing. Additional information regarding preventing tax related identity theft can be found at: http://www.irs.gov/uac/Identity-Protection. In addition to the above, we also recommend that you take additional steps with agencies outside of the IRS, and report incidents of identity theft to the Federal Trade Commission and contact the fraud departments of the three major credit bureaus listed above.