McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

McDonald Hopkins
A business advisory and advocacy law firm®

March 1, 2024

VIA U.S. MAIL

John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Arsenault and Cline – Incident Notification

Dear Mr. Formella,

McDonald Hopkins PLC represents Arsenault and Cline CPA's Inc (Arsenault and Cline) (located at 150A Andover St #7a, Danvers, MA 01923). I am writing to provide notification of an incident at Arsenault and Cline that may affect the security of personal information of fifteen (15) New Hampshire residents. By providing this notice, Arsenault and Cline does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On July 10, 2023, Arsenault and Cline identified suspicious activity potentially associated with two employee email accounts. After discovering the incident, Arsenault and Cline engaged our firm and third-party independent cybersecurity experts to conduct a thorough investigation of the nature and scope of the incident. Arsenault and Cline recently concluded its investigation, which revealed that an unauthorized actor gained access to two (2) of its employees' email accounts, and as a result, potentially viewed personal information. On February 6, 2024, after concluding an extensive forensic investigation and comprehensive review, Arsenault and Cline discovered that certain personal information was included within the data that may have been viewed by the unauthorized actor. The personal information contained within the impacted data included

. The types of impacted information varied by individual.

Arsenault and Cline wanted to inform you (and the affected residents) of the incident and explain the steps that it is taking to help safeguard the affected residents against identity fraud. Arsenault and Cline is providing the affected residents with written notification of this incident commencing on or about March 1, 2024 in substantially the same form as the letter attached hereto. Arsenault and Cline is offering the affected residents whose were potentially impacted complimentary memberships with a credit monitoring service.

Arsenault and Cline is advising the affected resident about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Arsenault and Cline, protecting the privacy of personal information is a top priority. Arsenault and Cline is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Arsenault and Cline continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at . Thank you for your cooperation.

Sincerely,

James J. Giszczak

Encl.

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]:

We are writing to inform you of a data security incident at Arsenault and Cline CPA's Inc. ("Arsenault and Cline") involving some of your information. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about July 10, 2023, we identified suspicious activity involving two of our employee email accounts.

What We Are Doing

Upon learning of the issue, our technology team acted quickly to mitigate the incident and ensure the security of our systems. We also commenced a prompt and thorough investigation. As part of our investigation, Arsenault and Cline has been working very closely with external cybersecurity professionals experienced in handling these types of incidents.

Based on the results of the forensic investigation, it was determined that two Arsenault and Cline email accounts were likely subject to unauthorized access beginning on June 23, 2023. At that time, we conducted a comprehensive review of the impacted data. On February 6, 2024, our extensive forensic investigation and manual document review concluded and determined that certain personal information was included within the impacted mailbox data that may have been viewed or acquired as a result of the incident.

What Information Was Involved

The impacted data contained your [redacted].

What You Can Do

We are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in 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.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements, explanation of benefits 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.

For More Information

Please accept our apologies that this incident occurred. We are 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 and internal controls 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 on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you 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 charge. 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 contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

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 your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

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.

If this notice letter states that your financial account information and/or credit or debit card 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.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

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.