McDonald Hopkins
A business advisory and advocacy law firm®

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

P 1.248.646.5070
F 1.248.646.5075

April 11, 2024

VIA U.S. MAIL

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Brown Paindiris & Scott, LLP – Incident Notification

Dear Attorney General John Formella:

McDonald Hopkins PLC represents Brown Paindiris & Scott, LLP ("Brown Paindiris & Scott"). I am writing to provide notification of an incident at Brown Paindiris & Scott that may affect the security of personal information of two (2) New Hampshire residents. Brown Paindiris & Scott's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Brown Paindiris & Scott does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Brown Paindiris & Scott recently discovered that an unauthorized actor briefly and temporarily obtained access to one employee email account. Upon learning of this issue, Brown Paindiris & Scott immediately began efforts to remediate the issue and commenced a prompt and thorough investigation. As part of their investigation, Brown Paindiris & Scott has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, Brown Paindiris & Scott discovered on March 18, 2024, that the impacted email account that was accessed between November 7, 2023 and November 9, 2023 contained a limited amount of personal information, including the affected residents'

. Not all data elements were impacted for each resident.

Brown Paindiris & Scott wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Brown Paindiris & Scott is providing the affected residents with notification of this incident commencing on or about April 11, 2024 in substantially the same form as the letter attached hereto. Brown Paindiris & Scott is providing the affected residents with of complimentary credit monitoring services and is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular

basis. Brown Paindiris & Scott is advising the affected residents about the process for placing a fraud alert and/or security freeze 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 Brown Paindiris & Scott, protecting the privacy of personal information is a top priority. Brown Paindiris & Scott is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Brown Paindiris & Scott continually evaluates and modifies its practices and internal controls to enhance the security and privacy of the personal information.

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

Very truly yours,

Nicholas A. Kurk

Encl.

Brown Paindiris & Scott, LLP

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

[redacted]

[redacted]

[redacted]

Dear [redacted],

The privacy and security of the personal information we maintain is of the utmost importance to Brown Paindiris & Scott, LLP ("Brown Paindiris & Scott"). We are writing with important information regarding a recent data security incident that involved some of your information. We want 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?

We recently learned that an unauthorized actor briefly and temporarily obtained access to one employee email account.

What We Are Doing.

Upon learning of this issue, Brown Paindiris & Scott immediately began efforts to remediate the issue and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on March 18, 2024, that the impacted email account that was accessed between November 7, 2023 and November 9, 2023 contained some of your personal information.

What Information Was Involved.

The impacted email account contained some of your personal information, including your [redacted]

What You Can Do.

We have no evidence that any of your information has been used for financial fraud or identity theft as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Identity Defense Complete credit and identity monitoring. For more information on identity theft prevention and the credit monitoring product being offered to you, including instructions on how to activate your complimentary [redacted] month membership, please see the additional information provided in this letter.

This letter also provides other 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. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

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 further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 am to 9 pm Eastern Time.

Sincerely,

Brown Paindiris & Scott, LLP.
2252 Main St.
Glastonbury, CT 06033

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary [redacted] Month Credit Monitoring.**

Identity Defense

[redacted]
Enter your Activation Code: [redacted]
Enrollment Deadline: [redacted]
Service Term: [redacted] Months

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

To enroll in Identity Defense, visit [redacted]

1. Enter your unique Activation Code [redacted]
   Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is [redacted] After [redacted] the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by** [redacted] **you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at [redacted]

2. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary [redacted] month credit monitoring services, we recommend that you place an initial one-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

3. 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.

4. 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.

5. 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.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

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.