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

Christine Czuprynski
Direct Dial: 248.220.1360
E-mail: cczuprynski@mcdonaldhopkins.com

August 31, 2022

VIA U.S. MAIL

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

Re: Rawle & Henderson, LLP – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents the Rawle & Henderson, LLP ("Rawle & Henderson"). I am writing to provide notification of an incident at Rawle & Henderson that may affect the security of personal information of approximately one (1) New Hampshire resident. Rawle & Henderson'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, Rawle & Henderson does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On February 25, 2022, Rawle & Henderson experienced a cybersecurity incident involving ransomware. Upon learning of this issue, Rawle & Henderson immediately contained the threat by disabling all unauthorized access to the network and immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine the extent of any compromise of the information on its network. Based on its comprehensive investigation and document review, Rawle & Henderson concluded on July 22, 2022 that a limited amount of personal information was accessed or acquired in connection with this incident. This information included the affected resident's full name and Social Security number.

To date, Rawle & Henderson is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Rawle & Henderson wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Rawle & Henderson is providing the affected resident with written notification of this incident commencing on or about August 24, 2022 in substantially the same form as the letter attached hereto. Rawle & Henderson is offering the affected resident a complimentary one-year membership with a credit monitoring service. Rawle & Henderson is advising the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Rawle & Henderson is advising the affected resident about the process for placing fraud alerts

and/or security freezes on his/her credit files and obtaining free credit reports. The affected resident is being advised to contact his/her financial institutions to inquire about steps to take to protect their accounts. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Rawle & Henderson, protecting the privacy of personal information is a top priority. Rawle & Henderson is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. In response to this incident, Rawle & Henderson strengthened its network and implemented additional security improvements recommended by third-party cyber security experts, including resetting account passwords and strengthening its password security policies, ensuring compliance with multi-factor authentication for network access, upgrading its firewall, and deploying endpoint detection software. Rawle & Henderson 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 (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

Christine N. Czuprynski

Encl.

RAWLE & HENDERSON LLP

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

[redacted]

[redacted]

We are writing to provide information regarding a security incident. The privacy and security of the personal information we maintain is of the utmost importance to Rawle & Henderson. We wanted to provide you with information about the incident, explain the services we have made available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

Rawle & Henderson experienced a cybersecurity incident involving ransomware. Upon learning of this issue, we quickly contained the threat by disabling all unauthorized access to the network and immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine the extent of any compromise of the information on our network. Based on our comprehensive investigation and document review, we concluded on July 22, 2022 that your personal information may have been accessed or acquired in connection with this incident.

What Information Was Involved?

The potentially acquired information included your personal information, specifically your [redacted]

What You Can Do.

To date, we are not aware of any misuse of your information as a result of this incident. Out of an abundance of caution, however, we wanted to update you on the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well. To protect you from potential misuse of your information, we are offering a complimentary <<CM Length>>-month membership of myTrueIdentity from TransUnion. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. For more information on identity theft prevention and myTrueIdentity, including instructions on how to activate your complimentary <<CM Length>>-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.

Please accept our apologies that this attack happened. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. In response to this incident, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts, including resetting account passwords and strengthening our password security policies, ensuring compliance with multi-factor authentication for network access, upgrading our firewall, and deploying endpoint detection software.

[redacted]

If you have any further questions regarding [redacted] 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 [redacted]

Sincerely,

Executive Committee
Rawle & Henderson LLP
The Widener Building | 1339 Chestnut Street, 16th Floor
Philadelphia, PA 19107

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary <<CM Length>>-Month Credit Monitoring.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at [redacted] and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at [redacted]. When prompted, enter the following 6-digit telephone pass code [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and [redacted] Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: [redacted]

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary <<CM Length>>-month credit monitoring services, we recommend that you place an initial 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 105788
Atlanta, GA 30348
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 LLC
P.O. Box 6790
Fullerton, PA 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

3. 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
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960

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

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
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.

[redacted]

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 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 this letter indicates that your financial account number was impacted, we recommend that you contact your financial institution to inquire about ways in which you can protect your account, including obtaining a new account number.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

[redacted]