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

February 15, 2021

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: The Richards Group – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents The Richards Group. I am writing to provide notification of an incident at The Richards Group that may affect the security of personal information of approximately 1,321 New Hampshire residents. The Richards Group'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, The Richards Group does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

The Richards Group learned that an employee email account was compromised by an email phishing attack resulting in unauthorized access to the email box. Upon learning of the issue, The Richards Group immediately secured the account and commenced a prompt and thorough investigation. As part of its investigation, The Richards Group has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual email review, The Richards Group discovered on August 21, 2020 that the impacted email account that was accessed between May 1, 2020, and May 11, 2020 contained individually identifiable personal information. Thereafter, The Richards Group worked diligently and comprehensively to identify each impacted individual, as well as the business customer to which each individual was associated. On November 24, 2020 The Richards Group completed its review and determined that a limited amount of personal information was impacted, including the affected residents' full names and one (1) or more of the following: Social Security numbers, driver's license numbers, tax identification numbers, other government-issued identification numbers, financial account information, credit or debit card information, and/or medical information.

To date, The Richards Group has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, The Richards Group 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. The Richards Group is providing the affected residents with written notification of this incident commencing on or about January 20, 2021 in substantially the same form as the letter attached hereto. The Richards Group is offering the affected residents whose Social Security numbers were impacted complimentary memberships with a credit monitoring service. The Richards Group is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents whose financial account information and/or credit or debit card information was impacted are being advised to contact their financial institutions to inquire about steps to take to protect their accounts. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. The affected residents whose medical information was impacted are also being provided steps to take to safeguard themselves against medical identity theft.

Notification of this matter has also been provided to the U.S. Department of Health and Human Services Office for Civil Rights, in compliance with 45 CFR §§ 164.400-414. The Richards Group operates as a business associate for several covered entities, and data relating to the New Hampshire residents was subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191.

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

Should you have any questions concerning this notification, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Christine Czuprynski

Encl.

The Richards Group

[RETURN ADDRESS]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

[redacted]

Dear [redacted]:

We are writing with important information regarding a security incident. The privacy and security of the personal information we maintain is of the utmost importance to The Richards Group ("Richards Group"). The Richards Group provides insurance-related services to businesses, including your current or former employer. 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?

We learned that a Richards Group employee email account was compromised by an email phishing attack resulting in unauthorized access to the email box.

What We Are Doing.

Upon learning of the issue, we immediately secured the account 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 email review, we discovered on August 21, 2020 that the impacted email account that was accessed between May 1, 2020, and May 11, 2020 contained individually identifiable personal information.

Thereafter, we worked diligently and comprehensively to identify each impacted individual, as well as the business customer to which each individual was associated. On November 24, 2020 we completed our review and determined that your personal information was impacted. The Richards Group was in possession of certain elements of your personal information in order to provide insurance-related services to your current or former employer, or to provide such services directly to you. Some of that information was contained within the accessed email account. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

The accessed email account contained some of your personal information, specifically your [redacted]

What You Can Do.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. 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. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year 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 account statements for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we have offered suggestions for protecting your medical information.

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 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, 9am to 9pm Eastern Time.

Sincerely,

[redacted]

The Richards Group

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [redacted]
3. PROVIDE the **Activation Code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at [redacted]
or call [redacted] to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted].

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. 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 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
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

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

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 sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

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 monitoring 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.

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 states that your financial account information and/or credit/debit card account information was impacted, we recommend that you notify your financial institution to inquire about ways in which you can protect your financial or credit card account(s), including by obtaining new account numbers.

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, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

6. Protecting Your Medical Information.

If this notice letter states that your medical information was impacted, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.

- 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.