

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

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

P 1.248.646.5070
F 1.248.646.5075

RECEIVED

FEB 11 2022

CONSUMER PROTECTION

February 8, 2022

VIA U.S. MAIL

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

Re: Caulipower, LLC – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents Caulipower, LLC (“Caulipower”). I am writing to provide notification of an incident that may affect the security of personal information of one (1) New Hampshire resident. Caulipower’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, Caulipower does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Caulipower recently learned that an unauthorized individual obtained access to a limited number of employee email accounts between July 11, 2021 and July 19, 2021. Upon learning of this issue, Caulipower immediately commenced a prompt and thorough investigation. As part of this investigation, Caulipower has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Caulipower devoted considerable time and effort to determine what information was contained in the affected email accounts. Based on its comprehensive investigation and manual document review, Caulipower discovered on January 12, 2022 that the compromised email accounts contained a limited amount of personal information, including the affected resident’s full name and driver’s license number.

At the time of this notification, Caulipower is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Caulipower 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. Caulipower is providing the affected resident with written notification of this incident commencing on or about February 8, 2022 in substantially the same form as the letter attached hereto. Caulipower will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Caulipower will advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

February 8, 2022

Page 2

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

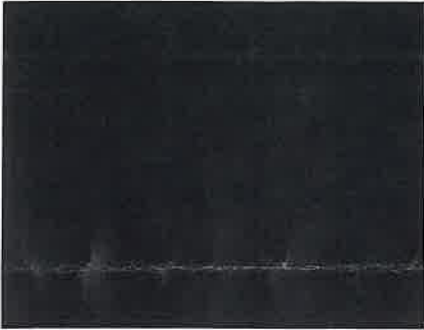
Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Dominic A. Paluzzi

DAP/bg
Enclosure



Dear [REDACTED]:

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Caulipower, LLC ("Caulipower"). As such, we wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that an unauthorized individual may have obtained access to a limited number of Caulipower employee email accounts.

What We Are Doing.

Upon learning of the issue, we immediately 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 January 12, 2022 that the impacted email accounts that may have been accessed between July 11, 2021 and July 19, 2021 contained some of your personal information. 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 impacted email accounts contained some of your personal information, specifically your [REDACTED]. [REDACTED]

What You Can Do.

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. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis.

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. Since this incident, we have reset passwords, implemented a robust endpoint detection response tool, and worked with an external cybersecurity firm to further harden our network security.

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 [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,

[REDACTED]

- OTHER IMPORTANT INFORMATION -

1. Placing a Fraud Alert on Your Credit File.

You may 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, CA 92834

<https://www.transunion.com/fraud-alerts>

(800) 680-7289

2. 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.equifax.com/personal/credit-report-services/credit-freeze/>

1-800-349-9960

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/credit-freeze>

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.

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.

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.