

James J. Giszczak  
Direct Dial: 248-220-1354  
E-mail: [jgiszczak@mcdonaldhopkins.com](mailto:jgiszczak@mcdonaldhopkins.com)

RECEIVED

JUL 26 2022

CONSUMER PROTECTION

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

P 1.248.646.5070  
F 1.248.646.5075

July 22, 2022

**VIA U.S. MAIL**

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

**Re: GMES Electric Supply – Incident Notification**

Dear Mr. Formella:

McDonald Hopkins PLC represents GMES Electric Supply, Inc. ("GMES"). I am writing to provide notification of an incident at GMES that may affect the security of personal information of two (2) New Hampshire residents. By providing this notice, GMES does not waive any rights or defenses.

On January 28, 2022, GMES learned that an unauthorized individual may have obtained access to two employee email accounts. Upon learning of the issue, GMES immediately began efforts to remediate the issue and commenced a prompt and thorough investigation. As part of its investigation, GMES 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, GMES discovered on June 8, 2022 that one of the impacted email accounts potentially accessed between January 25, 2022 and January 30, 2022 contained some personal information.

GMES has no indication that any of the information has been misused for purposes of identity theft. Nevertheless, out of an abundance of caution, GMES wanted to inform you of the incident. GMES is providing written notification of this incident to affected residents commencing on July 22, 2022, in substantially the same form as the notice letter enclosed herein. GMES is offering the affected residents complimentary one-year membership with a credit monitoring service. GMES is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. GMES 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 GMES, protecting the privacy of personal information is a top priority. GMES is committed to maintaining the privacy of personal information in its possession and has taken

July 22, 2022

Page 2

many precautions to safeguard it. GMES 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) 220-1354 or [jgiszczak@mcdonaldhopkins.com](mailto:jgiszczak@mcdonaldhopkins.com). Thank you for your cooperation.

Sincerely,

James J. Giszczak



**IMPORTANT INFORMATION  
PLEASE REVIEW CAREFULLY**

Dear [REDACTED]

We are writing with important information regarding a recent cyber incident that occurred. The privacy and security of the personal information we maintain is of the utmost importance to Green Mountain Electric Supply, Inc. ("GMES"). 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 help protect your information.

**What Happened?**

On January 28, 2022, GMES learned that an unauthorized individual may have obtained access to two employee email accounts.

**What We Are Doing.**

Upon learning of the issue, we 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 June 8, 2022 that one of the impacted email accounts potentially accessed between January 25, 2022 through January 30, 2022 contained some of your personal information.

**What Information Was Involved?**

The impacted email account contained some of your personal information, specifically your [REDACTED]

**What You Can Do.**

**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. To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. These services are completely free to you, and activating them will not hurt your credit score. **For more information on your identity monitoring services, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the pages that follow this letter.**

This letter also provides other precautionary measures you can take to help 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. To the extent that it is helpful, we have also provided information about how to help protect 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. Since this incident, we have reset passwords, implemented multi-factor authentication, 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 at [REDACTED]** This response line is staffed with professionals familiar with this incident. The response line is available Monday through Friday, 9:00 am to 6:30 pm ET, excluding major U.S. holidays.

Sincerely,

Green Mountain Electric Supply, Inc.

– OTHER IMPORTANT INFORMATION –

1. **Activating your Complimentary 12-Month Identity Monitoring.**



**Article I. TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until [REDACTED] to activate your identity monitoring services.

Membership Number: [REDACTED]

You have been provided with access to the following services from Kroll:

**Section I.01 Triple Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

**Section I.01 Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Section I.01 Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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  
<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**  
Fraud Victim Assistance  
Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<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 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/>  
(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  
<http://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 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 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](http://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](http://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.

#### **6. Protecting Your Medical Information.**

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, 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.

**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/](http://www.ncdoj.gov/), Telephone: 877-566-7226.