

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

RECEIVED

APR 18 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

April 13, 2022

VIA U.S. MAIL

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

Re: Rokstad Power Inc. – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents Rokstad Power Inc. I am writing to provide notification of an incident at Rokstad Power Inc. that may affect the security of personal information of approximately one (1) New Hampshire resident. The investigation of Rokstad Power Inc. 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, Rokstad Power Inc. does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

A hard drive was stolen from a site trailer on one of our project sites on March 5, 2022. Upon learning of this issue, Rokstad Power, Inc. immediately notified law enforcement of the incident and launched an investigation. As part of its investigation, Rokstad Power, Inc. has been working with outside data privacy professionals who regularly investigate and analyze these types of situations. Rokstad Power, Inc. discovered on March 14, 2022 that the stolen hard drive contained a limited amount of personal information, including the affected resident's full name, Social Security number, date of birth, financial account information, driver's license number and/or passport number, user account and password information, and digital signature.

Rokstad Power Inc. has no indication that any information has been misused. Nevertheless, out of an abundance of caution, Rokstad Power Inc. 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. Rokstad Power Inc. is providing the affected resident with notification of this incident commencing on or about April 13, 2022 in substantially the same form as the letter attached hereto. Rokstad Power Inc. is advising the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Rokstad Power Inc. is providing the resident with a complimentary 12 months of credit monitoring and is advising 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 are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

April 13, 2022
Page 2

At Rokstad Power Inc., protecting the privacy of personal information is a top priority. Rokstad Power Inc. is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Rokstad Power Inc. 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) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,



James J. Giszczak

Encl.

ROKSTAD

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 Rokstad Power Inc. 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 protect your information.

What Happened?

On March 5, 2022, a hard drive was stolen from a site trailer on one of our project sites.

What We Are Doing.

Upon learning of this theft, we immediately notified law enforcement of the incident and launched an investigation. As part of our investigation, we have been working with outside data privacy professionals who regularly investigate and analyze these types of situations. We discovered on March 14, 2022 that the stolen hard drive 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 stolen hard drive contained some of your personal information, [REDACTED]
[REDACTED]
[REDACTED]

What You Can Do.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Equifax Credit Watch™ Gold. For more information on identity theft prevention and Equifax Credit Watch™ Gold, 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.

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 [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. Enrolling in Complimentary 12-Month Credit Monitoring.

Enter your Activation Code: [REDACTED]

Enrollment Deadline: [REDACTED]

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to [REDACTED]

Enter your unique Activation Code of [REDACTED] then click “Submit” and follow these 4 steps:

1. Register:

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. Create Account:

Enter your email address, create a password, and accept the terms of use.

3. Verify Identity:

To enroll in your product, we will ask you to complete our identity verification process.

4. Checkout:

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded. ²The Automatic Fraud Alert feature is made available to consumers by Equifax

Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. 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 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

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/>
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 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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164

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/, Telephone: 877-566-7226.

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.