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

Colin M. Battersby
Direct Dial: 248-593-2952
E-mail: cbattersby@mcdonaldhopkins.com

May 11, 2020

VIA U.S. MAIL

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

Re: Exeter Health Resources, Inc. – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Exeter Health Resources, Inc., Exeter Hospital, Inc., Core Physicians, LLC, and Rockingham Visiting Nurse Association and Hospice (collectively "Exeter"). I am writing to provide notification of an incident that may affect the security of personal information of approximately four thousand four hundred eighty-three (4,483) New Hampshire residents. Exeter'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, Exeter does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Exeter utilizes PaperlessPay to issue electronic pay stubs and annual Federal tax forms, such as W2s. On March 20, 2020, PaperlessPay advised Exeter that, on February 19, 2020, federal law enforcement personnel contacted PaperlessPay and reported an unknown person was purporting to sell "access" to PaperlessPay's client database on the dark web. In response, PaperlessPay shut down its servers and forced password changes. As Exeter understands it, PaperlessPay continues to work with law enforcement and external forensic experts in investigating the incident.

Based on the forensic investigation of PaperlessPay's information systems conducted thus far, however, PaperlessPay has confirmed that an unknown person gained access to PaperlessPay's servers where Exeter employees' data was stored. While the available evidence has not allowed PaperlessPay to determine what data the person may have accessed or viewed, it is possible some or even all of the affected residents' personal information was accessed or viewed. The information included the affected residents' full names, residential addresses, as both appear on pay stubs, Social Security numbers, and bank account numbers (but not routing numbers), as well as other information necessary to generate pay stubs and Federal tax forms.

Exeter is not presently aware of any misuse of information arising out of this incident. Nevertheless, out of an abundance of caution, Exeter 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. Exeter is providing the affected residents with written notification of this incident commencing on or about May 8, 2020 in substantially the same form as the letter attached hereto. Exeter is offering the affected residents complimentary one-year memberships with a credit monitoring service. Exeter 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 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.

PaperlessPay has informed Exeter that it has secured its network to prevent future incidents. PaperlessPay rebuilt new servers, assigned new IP addresses to all the new servers, changed all passwords for users and administrators, and disabled all remote access capabilities to the new servers.

Exeter takes the protection of employee personal information very seriously. Before this incident, PaperlessPay had been a reliable vendor for over eight (8) years.

Should you have any questions concerning this notification, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Colin M. Battersby

Encl.

EXETER HEALTH RESOURCES
The Art of Wellness

[redacted]

[redacted]

[redacted]

Dear [redacted]

We are writing with important information regarding a recent data security incident at one of our third-party vendors, PaperlessPay Corporation ("PaperlessPay"), which operates the MyE-Stub website. Exeter Health Resources, Inc., Exeter Hospital, Inc., Core Physicians, LLC, and Rockingham Visiting Nurse Association and Hospice (collectively "Exeter") utilize PaperlessPay to issue electronic pay stubs and annual Federal tax forms, such as W2s. Because the personal information provided to PaperlessPay to provide these services may have been accessible to an unauthorized person, we want to provide you with information about the incident at PaperlessPay, explain the services Exeter is making available to you, and let you know that we continue to take significant measures to help protect your information.

What Happened?

On February 20, 2020, Exeter employees experienced difficulty in accessing PaperlessPay's site to view pay stub information. PaperlessPay communicated its site was down due to unscheduled maintenance that was taking longer than anticipated. Exeter subsequently made multiple inquiries about the status of PaperlessPay's site. Not having received a response to these inquiries, Exeter made the decision to stop sending payroll data files to PaperlessPay and internally process pay stub and Federal tax forms. The last payroll data file sent to PaperlessPay was on February 18 for the February 20 pay date.

On March 20, 2020, PaperlessPay officially advised Exeter that, on February 19, 2020, federal law enforcement personnel contacted PaperlessPay and reported an unknown person was purporting to sell "access" to PaperlessPay's client database on the dark web. In response, PaperlessPay shut down its servers and forced password changes. As we understand it, PaperlessPay continues to work with law enforcement and external forensic experts in investigating the incident.

Based on the forensic investigation of PaperlessPay's information systems conducted thus far, however, PaperlessPay has confirmed that an unknown person gained access to PaperlessPay's servers where Exeter employees' data was stored. While the available evidence has not allowed PaperlessPay to determine what data the person may have accessed or viewed, it is possible some of your personal information was accessed or viewed.

What Personal Information Did PaperlessPay Have?

Exeter provided PaperlessPay with your full name and residential address, as both appear on your pay stub, Social Security number, and bank account number (but not the bank's routing number), as well as other information necessary to generate your pay stubs and Federal tax forms.

What You Can Do.

To help protect you and your personal information, 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 personal information. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Additional information describing these services, including how to activate your complimentary one-year membership, is included with this letter.

Also provided in "Other Important Information" are 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. Because your bank account information may have been accessed, we recommend you contact your financial institution to discuss steps you can take to help protect your account, including whether you should close it or obtain a new account number. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

What is PaperlessPay Doing?

PaperlessPay has informed Exeter that it has secured its network to prevent future incidents. PaperlessPay rebuilt new servers, assigned new IP addresses to all the new servers, changed all passwords for users and administrators, and disabled all remote access capabilities to the new servers.

For More 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 about what you can do to help protect against misuse of your information, and is available Monday through Friday, [redacted].

We take the safeguarding of employee's personal information very seriously. Before this incident, PaperlessPay had been a reliable vendor for over eight (8) years. We are sorry that this has happened.

Sincerely,

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Take Advantage of Your Identity Monitoring Services

Visit [redacted] to activate and take advantage of your identity monitoring services.
You have until [redacted] *to activate your identity monitoring services.*
Membership Number: [redacted]

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data —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 can help you determine if it's an indicator of identity theft.

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.

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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

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 12-month "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	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. Consider 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	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/
1-800-349-9960	1-888-397-3742	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 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.

[1] 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.

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.