150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

May 26, 2020

Michael J. Waters
(312) 463-6212
mwaters@polsinelli.com

Via Email (ATTORNEYGENERAL@DOJ.NH.GOV)

Attorney General Gordon J. MacDonald
Office of the Attorney General
Attn: Security Incident Notification
33 Capitol Street
Concord, NH 03301

Re: Notification of a Computer Security Incident Involving Personal Information Pursuant to N.H. Rev. Stat. § 359-C:20

Dear Attorney General MacDonald:

We represent Emerson Hospital ("Emerson") in connection with an incident that involved the personal information of 136 New Hampshire residents, and provide this notice on behalf of Emerson pursuant to N.H. Rev. Stat. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Emerson is notifying you of this incident, Emerson does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY INCIDENT OR UNAUTHORIZED ACCESS

On or around March 20, 2020, PaperlessPay Corporation ("PPC") notified Emerson of a security incident that it recently experienced. Emerson contracts with PPC for the provision of online paystubs and W-2 tax forms. According, to PPC, on February 19, 2020, the Department of Homeland Security ("DHS") contacted PPC and notified it that someone was purporting to sell access to PPC's client database on the dark web. PPC shut down its web server and SQL server and implemented additional security controls. PPC worked with DHS and the Federal Bureau of Investigation ("FBI") and retained a cybersecurity firm to conduct a forensic investigation. PPC has not provided Emerson any additional information on the progress or outcome of the investigation. Upon receiving notification from PPC, Emerson immediately stopped sending data to PPC, and cancelled its contract with PPC. Emerson and PPC are working together to obtain additional information concerning the incident, including what, if any information the threat-actor may have acquired.

At this point, Emerson is not aware of an unauthorized access or acquisition of its employees' personal information or that any of the information has been misused. However, PPC could not definitely rule out the possibility that someone accessed or acquired Emerson's employees' personal information. Accordingly, Emerson is notifying the potentially impacted employees and arranged for complementary identity theft protection services for the employees.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Emerson determined that 136 New Hampshire residents may have been impacted by this incident. Emerson is notifying the impacted individuals of the situation by letter today. Enclosed is a copy of the notice that is being sent to the impacted individuals.

STEPS TAKEN RELATING TO THE INCIDENT

Upon becoming aware of the incident, Emerson promptly investigated the incident to determine what, if any, personal information a third party might have acquired during the incident. Emerson is also providing complimentary identity theft protection services to the impacted individuals through Experian.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,

Michael J. Waters

Enclosure

Emerson Hospital
133 Old Road to Nine Acre Corner
Concord, MA 01742

May 26, 2020

[redacted]

Dear [redacted],

We are sending this letter to you as part of Emerson Hospital's commitment to data privacy and information security. We take data privacy and security very seriously, and it is important to us that you are notified of an incident involving your personal data.

On February 20, 2020, we received an email from Paperless Pay Corporation (PPC), which provides online paystub and W2 access for Emerson Hospital employees. In this email, we learned that the online "my-estub" service was not available due to an unspecified security incident. We subsequently learned from PPC that an unauthorized individual accessed their client database and attempted to sell that access on the web. The offer was detected by the Department of Homeland Security (DHS), and PPC immediately took their site offline and implemented additional security controls. PPC cooperated in a joint investigation conducted by DHS and the Federal Bureau of Investigation and retained a computer forensics firm to assist in its own internal investigation of the incident.

Since receiving notification from PPC, Emerson Hospital immediately stopped sending data to PPC and has terminated its contract. We have been working to obtain additional information from PPC about the nature of the event to determine the risk to your personal data.

In a letter dated March 20, 2020, PPC confirmed that an unknown person did gain access to its server the day before it was contacted by DHS, but was unable to determine what, if any, data the person may have accessed or viewed while connected to the server. If information was accessed, it could have included name, address, salary information and social security number. The data on the server was stored in different tables using ID numbers, not names, and would have required additional steps to associate the data with an individual. PPC had an alert system that designed to detect data file transfers, and no alert was triggered during this security incident. PPC has not provided Emerson any more information on the progress or outcome of the investigation.

Although there is no evidence that your information was accessed, the possibility of unauthorized access cannot be ruled out. As the protection of your personal information is important to us, we are offering you a complimentary two-year membership of Experian IdentityWorks^{SM} Credit 3B. This service 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. 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 two-year membership, please see the additional information provided in this letter.

We regret that our vendor experienced this unfortunate incident. We will continually work to protect the privacy and security of your information. For further information and assistance, please call 978-371-5395 from 9:00 a.m. to 5:00 p.m. ET Monday through Friday.

Sincerely,

[redacted]

To help protect your identity, we are offering a **complimentary** two-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

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: **https://www.experianidworks.com/3bcredit**
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 877-288-8057. 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 https://www.experianidworks.com/3bcredit
or call 877-288-8057 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 877-288-8057.

* 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.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:
1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected seven (7) Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).