

Joshua P. Brian
T: (850) 205-3336 F: (850) 681-9792
joshua.brian@nelsonmullins.com

215 South Monroe Street, Suite 400
Tallahassee, FL 32301
T: 850.681.6810 F: 850.681.9792
nelsonmullins.com

June 26, 2020

Via Certified Mail and E-Mail To: attorneygeneral@doj.nh.gov

Attorney General Gordon J. MacDonald
33 Capitol Street
Concord, NH 03301

RE: Notice of Data Breach by Third Party Vendor PaperlessPay Corporation

Dear Attorney General MacDonald:

Our law firm, Nelson Mullins Riley & Scarborough LLP, 215 South Monroe Street, Ste. 400, Tallahassee, FL 32301, represents Milford Regional Medical Center (“MRMC”), 14 Prospect Street, Milford, MA 01757, a multidisciplinary medical group. On March 20, 2020, MRMC received a Notice of Data Privacy Incident from PaperlessPay Corporation (“PaperlessPay”), a third-party vendor who hosted MRMC’s current and former employee paystub and W2 tax forms.

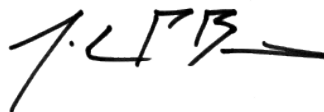
PaperlessPay represented that the Department of Homeland Security contacted it on February 19, 2020, based upon a dark web forum advertisement selling access to PaperlessPay’s SQL database server that contained MRMC’s current and former employees’ bank account numbers and Social Security numbers.

PaperlessPay represented that it engaged a forensic investigation firm that confirmed, at a minimum, that an unauthorized individual entered the server on February 18, 2020, and possibly staged data for exfiltration from the server.

As a result of PaperlessPay’s disclosures, MRMC decided to provide notice with an offer of identity monitoring without cost to its current and former employees. The sixteen (16) potentially impacted residents will be notified by the enclosed letter post-marked June 26, 2020, and be provided an offer of one (1) year of identity monitoring without cost.

Please let me know if you have any additional questions regarding this notification.

Very truly yours,



Joshua P. Brian

June 26, 2020

Page 2

Enclosures: Notice to New Hampshire Residents
PaperlessPay Notice of Data Privacy Incident

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Milford Regional Medical Center, Inc. (“Milford Regional”) respects the privacy of your information, which is why we are writing to tell you about a data security incident by our former third-party paystub and W2 vendor, PaperlessPay Corporation (“PaperlessPay”), that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of PaperlessPay’s data security incident.

What Happened

On March 20, 2020, PaperlessPay provided notice to Milford Regional that an unauthorized individual gained access to its server that hosts your paystub and W2 data (“payroll data”). Although PaperlessPay was unable to substantiate the extent of the access, it did confirm that an unauthorized individual gained access to its server at least once on February 18, 2020, and that the unauthorized individual had the ability to query any payroll data within the server.

PaperlessPay could not confirm that any of your payroll data was accessed or acquired by an unauthorized individual from within its database, but was unable to eliminate the possibility. Because we take the protection of your personal information very seriously, we are providing you with notice of the possible unauthorized disclosure and one (1) year of identity monitoring at no cost to you to allow you to take steps to protect your personal information.

What Information Was Involved

PaperlessPay was unable to confirm whether your information was actually accessed or acquired by an unauthorized individual. However, as a result of this incident, some of your personal information may have been accessed and/or acquired without authorization, including your first and last name, <<Breached Elements>>.

We are notifying you so you can take appropriate steps to protect your personal information.

What We Are Doing

To help relieve concerns following this incident, we have secured TransUnion to provide identity monitoring at no cost to you for one (1) year. TransUnion is an industry leader and functions as a first point of contact for credit-related issues, which allows it to efficiently furnish timely notification about credit-related issues to individuals enrolled in its identity monitoring service.

Visit www.MyTrueIdentity.com to activate and take advantage of your identity monitoring service.

You have until <<EnrollmentDate>> to activate your identity monitoring service.

myTrueIdentity Credit Monitoring Service Activation Code: <<ACTIVATION CODE>>

Additional information describing this service is included with this letter. We encourage you to review the description and to consider enrolling in this service.

Further, because of PaperlessPay's data event, we transitioned to an in-house solution to provide paystub and W2 services.

What You Can Do

Please review the enclosed "**Additional Resources**" information included with this letter, which describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

For further information, please call 855-917-3559 Monday through Friday, between 9:00 a.m. and 9:00 p.m. EST. We take the protection of your personal information very seriously and apologize for any inconvenience PaperlessPay's incident may cause you. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

James Papadakos

James Papadakos, Executive VP/CFO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, P.O. Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, P.O. Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, P.O. Box 34012, Fullerton, CA 92834, www.transunion.com, 1-800-916-8800

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity over the next twenty-four months, and immediately report incidents of suspected identity theft to both your financial provider and law enforcement.

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. You may also seek to have information relating to fraudulent transactions removed from your credit report. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont residents. You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report free of charge.

A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) legible copy of a government issued identification card; (6) legible copy of a recent utility bill or bank or insurance statement that displays your name and current mailing address, and the date of issue; and (7) any applicable incident report or complaint filed with a law enforcement agency.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>, 1-877-IDTHEFT (438-4338).

State Attorney General's Office Contact Information. <<Variable Data2>>.

Complimentary One-Year *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery.

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<**Insert Unique 12-letter Activation Code**>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<**Insert static 6-digit Telephone Pass Code**>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<**Enrollment Deadline**>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

[REDACTED]

From: mark.broughton@paperlesspaycorp.com
Sent: Friday, March 20, 2020 5:17 PM
To: [REDACTED]
Subject: Followup on Feb 20, 2020 Email

****EXTERNAL EMAIL** The e-mail below comes from a sender outside of MRMC. Please do not open attachments or click links from unknown or suspicious origin.**

Please BE EXTREMELY CAREFUL when reviewing external emails related to CORONAVIRUS. As always, with suspicious links & attachments ... **Think Before You Click!**



March 20, 2020

Electronic version sent to: [REDACTED]

Milford Regional Medical Center

[REDACTED]
14 PROSPECT STREET
MILFORD, MA 01757

Re: Notice of Security Incident

Dear [REDACTED]:

I am writing in follow up to the email I sent to our clients on February 20, 2020 about the recent data security incident at PaperlessPay Corporation (“PaperlessPay”). Since then, we have worked diligently to investigate the incident and we are now able to provide this summary report as promised in my email. As a third-party agent that maintains data on your behalf, we take this incident and the security of your data seriously.

What Happened?

On February 19, 2020, the Department of Homeland Security (“DHS”) contacted PaperlessPay and notified us that an unknown person was purporting to sell “access” to our client database on the dark web. In response, we shut down our web server and SQL server to prevent any potential unauthorized access. This interrupted our services to you and prevented your employees from accessing their payroll records for a short amount of time while the servers were offline.

Over the following weeks, we cooperated with the joint investigation conducted by DHS and the Federal Bureau of Investigation (“FBI”). Their investigation is ongoing, and we will continue to cooperate and help in any way we can. In addition, we retained the cybersecurity firm Ankura to help with our own, internal forensic investigation of the incident.

Through these investigations, we confirmed that an unknown person did gain access to our SQL server where your employees’ data is stored on February 18, 2020. The available evidence has not, however, allowed DHS, the FBI, or Ankura to determine what data the person may have accessed or viewed while connected to the SQL server. It is possible the person only used his access to determine the size of the SQL database and to stage it for subsequent access that he could sell to others, and that he did not directly access any employee data himself. However, he would have had the capability to run queries against the SQL database and view its data, so we cannot rule out the possibility of unauthorized access.

Page 2 of 2

What information was involved?

The information stored in our SQL server about your employees consists of the data components that appear on their pay stubs and tax forms, including their name, address, pay and withholdings, last four digits of bank account number (if your company includes that information on its pay stubs), and Social Security number. However, these data components are stored on the SQL server in different tables that are associated by user ID numbers, not names, within each table. Therefore, the only way to associate any data with an individual would be to run a query against the database and have it aggregate an individual’s name with his or her other data components.

What we are doing

In our capacity as a third-party agent that stores this employee data on your behalf, we are providing this supplemental notification, in addition to the one provided on February 24, to allow you to make any decisions about notification to your employees. We are committed to providing you with the information you need, so please contact us if you have other questions.

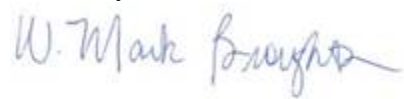
In the meantime, we have acted to secure our network and prevent future incidents. To resume our services, PaperlessPay rebuilt an entirely new domain controller, a new web server, and a new SQL server from scratch. We then restored database files to the new SQL server from backups. We assigned new IP addresses to all the new servers, changed all passwords for users and administrators, implemented a setting that requires clients to change their passwords when they login for the first time, and disabled all remote access capabilities to the new web server and SQL server.

We also installed an endpoint detection and response (EDR) application called Carbon Black on the new servers and other endpoints within our network. This has allowed us to monitor all activity while we completed this investigation of the incident. To date since Carbon Black has been running, there have been no indicators of compromise detected in the newly rebuilt environment, and we are pleased to report that all customer services are functioning as normal.

For more information

We are sorry for any concern or inconvenience this incident has caused or may cause you. For more information, please contact us at (800) 489-1711 ext. 422 or [REDACTED]

Sincerely,



W. Mark Broughton
CEO

This email has been scanned by the Symantec Email Security.cloud service.
For more information please visit [REDACTED]
