

November 3, 2023

VIA FIRST CLASS MAIL AND EMAIL

Honorable John Formella
New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
Office of the Attorney General
1 Granite Place South
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Data Breach Incident

Dear Attorney General Formella,

We represent PJ&A, which is incorporated as Perry Johnson & Associates, headquartered at 1489 W. Warm Springs, Suite 110, Henderson, NV 89012, in connection with a recent data incident. PJ&A is reporting this incident pursuant to N.H. Rev. Stat. § 359, on behalf of Northwell Health, Inc. (New Hyde Park, NY), Crouse Health (Syracuse, NY), and CarePoint Health (Hoboken, NJ). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While PJ&A is notifying you of this incident, PJ&A does not waive any rights or defenses relating to the incident or this notice.

NATURE OF THE INCIDENT

PJ&A provides medical transcription services, either directly or as a subcontractor to other contractors, to multiple health care organizations, including Northwell Health, Inc., Crouse Health, and CarePoint Health. In connection with those services, PJ&A collected certain personal information pertaining to patients of Northwell Health, Inc., Crouse Health, and CarePoint Health.

On May 2, 2023, PJ&A became aware of a potential data security incident impacting PJ&A's systems. An unauthorized actor claimed to have obtained access to company systems and data and demanded a ransom payment. Thereafter, PJ&A immediately launched an internal investigation and retained a cybersecurity vendor to assist with the investigation, contain the threat and further secure its systems.

Office of Attorney General Formella
November 3, 2023
Page 2

On May 22, 2023, PJ&A learned that the unauthorized party acquired certain information from PJ&A systems; the full extent of affected individuals and data required further investigation. PJ&A continued its investigation and ultimately determined that the unauthorized party had access to the PJ&A network between March 27, 2023, and May 2, 2023, and that the unauthorized party had access to servers with protected health information on April 7, 2023, and April 19, 2023. The investigation also determined that the unauthorized actor gained initial access to company systems by logging into an RDS Web application. It is unknown how the actor obtained the relevant login credentials.

PJ&A directed its external vendor to analyze the available backup files, determine their contents, and provide data sets that would identify all affected customers, individuals, and data elements. The analysis showed that the categories of personal information varied for each impacted individual, but generally included the following:

The final data sets were produced between September 28, 2023, and October 12, 2023. PJ&A then began working with Northwell Health, Inc., Crouse Health, and CarePoint Health to provide notifications to affected individuals.

NOTICE TO NEW HAMPSHIRE RESIDENTS

PJ&A and Northwell Health, Inc., Crouse Health, and CarePoint Health are providing notice to 867 residents of New Hampshire whose personal information was involved in the incident.* These notices are being made via letter mailed USPS First Class Mail beginning November 3, 2023. The notification letters include information on how to protect against fraudulent activity and identity theft and, where required by law, include an offer for complimentary credit monitoring and identity theft protection services. The notification letters also include a phone number for individuals to call with any questions they may have regarding the incident. Enclosed is a sample template of the notification letter.

STEPS TAKEN RELATING TO THE INCIDENT

Upon discovering the incident, initiated an internal investigation and engaged a leading forensic cybersecurity firm to assist in its investigation and to confirm the security of its computer systems. PJ&A also notified law enforcement. PJ&A is reviewing its information security policies and evaluating additional trainings and controls it can implement to reduce the risk of a similar incident occurring in the future. Finally, as discussed above, PJ&A is notifying the potentially involved

**WILSON
SONSINI**

Office of Attorney General Formella
November 3, 2023
Page 3

individuals, offering them complimentary credit monitoring as required by law, and providing them information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

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

Sincerely,

WILSON SONSINI GOODRICH &
ROSATI
Professional Corporation

/s/ Demian Ahn
Demian Ahn

cc: Covered Entities



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 3, 2023

K0005-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY



Re: **NOTICE OF DATA BREACH – PLEASE READ CAREFULLY**

Dear Sample A. Sample,

Perry Johnson & Associates, Inc. (“PJ&A,” “we,” or “us”) is providing this letter to inform you of an event that may affect your personal health information. This letter provides details of the event, our response, and resources available to you to help protect your personal health information from possible misuse, should you feel it is appropriate to do so.

Who Is PJ&A and Why Did We Have Your Information? PJ&A serves as a vendor to Northwell Health, Inc. and its subsidiaries and affiliates (collectively, “Northwell”). PJ&A provides certain transcription and dictation services to Northwell. In order to perform these services, PJ&A receives personal health information regarding Northwell patients.

What Happened. PJ&A became aware of a data security incident impacting our systems on May 2, 2023. We immediately initiated an investigation and engaged a cybersecurity vendor to further provide support in connection with our investigation and secure against potential system vulnerabilities. We promptly implemented the cybersecurity vendor-recommended actions to prevent the further disclosure of data as we continued to investigate the situation. Through our investigation, we determined that the unauthorized access to our systems occurred between March 27, 2023 and May 2, 2023, and the unauthorized access to Northwell patient data specifically occurred between April 7, 2023 and April 19, 2023.

On July 21, 2023, PJ&A notified Northwell that an unauthorized party had accessed and downloaded certain files from our systems. PJ&A had preliminarily determined that Northwell data was impacted on May 22, 2023 and, by September 28, 2023, confirmed the scope of the Northwell data impacted.

What Information Was Involved. We have confirmed that certain files containing your personal health information were impacted by this incident. Specifically, the following information may have been impacted:

What We Are Doing. We are committed to maintaining the privacy and security of your information and take this incident very seriously. PJ&A took, and will continue to take, appropriate steps to address this incident, including updating our systems to prevent incidents of this nature from occurring in the future. As soon as we learned of the unauthorized access to our systems, PJ&A immediately initiated an investigation and retained a cybersecurity vendor to assist with containing the threat and with further securing our systems. PJ&A notified law enforcement about the incident and continues to cooperate with law enforcement’s investigation. PJ&A further

implemented additional technical restrictions in our systems, and we required a password reset for all employees. Additionally, with the assistance of our cybersecurity vendor, we deployed an endpoint detection and response system to monitor any unauthorized access of our systems. PJ&A has taken additional steps to ensure that no patient data was made public, and, to date, we have not identified any evidence that the unauthorized actor has disclosed and/or made any observable use of the data.

What You Can Do. Northwell has arranged to have Experian IdentityWorksSM protect your identity for **one year** at no cost to you.

Experian IdentityWorksSM provides complimentary identity restoration and fraud detection services to you for one year. Please refer to the enclosed “Experian IdentityWorks Details” for further information and instructions for activating your one-year membership.

We also encourage you to regularly review your financial accounts and report any suspicious or unrecognized activity immediately. The enclosed “Important Identity Theft Information” provides further information about what you can do. As recommended by federal regulatory agencies, you should remember to be vigilant for the next _____ and report any suspected incidents of fraud to the relevant financial institution.

For More Information. The privacy and security of your personal health information is of the utmost importance to us. We sincerely regret this occurrence and apologize for any inconvenience or concern that it may cause you. Should you have any questions regarding the incident, please do not hesitate to contact us at _____ between 8:00 AM EST and 12:00 AM EST. If you have any questions regarding your credit monitoring or identity protection services, please call the number on the following page.

Sincerely,

Perry Johnson & Associates, Inc.

Enclosure

EXPERIAN IDENTITYWORKSSM DETAILS

Please note that Identity Restoration is available to you for **one year** from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at . Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent will be available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

ADDITIONAL DETAILS REGARDING YOUR ONE YEAR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** 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.
- **Lost Wallet:** Provides assistance with canceling/replacing lost or stolen credit, debit, and medical cards.
- **Child Monitoring:** For 10 children up to 18 years old, Internet Surveillance and monitoring to determine whether enrolled minors in your household have an Experian credit report are available. Also included are Identity Restoration and up to \$1M Identity Theft Insurance.**

Please note that you may find additional information regarding identity theft protection in the enclosed document.

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill; and
- 6) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity

theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
[www.experian.com/
fraud/center.html](http://www.experian.com/fraud/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
[www.transunion.com/fraud-
victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

State Specific Information

District of Columbia residents may contact the District of Columbia Attorney General at 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and <https://oag.dc.gov/>.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5926 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, calling the Identity Theft Unit at 1.410.576.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

New York residents may contact the New York Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/>, calling 1.919.716.6000 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <https://ago.vermont.gov/>.