



[REDACTED]



December 22, 2023

Notice of Data Incident

Dear [REDACTED]:

Parathon by JDA eHealth Systems (“Parathon”) is a third-party denials management company who is contracted with NorthShore University HealthSystem (“NorthShore”) to assist in challenging insurance denials and securing proper reimbursement to NorthShore and its patients for medical services. We are writing to inform you of an incident experienced by Parathon that may have exposed your personal information. NorthShore’s systems were not compromised. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

On July 27, 2023, Parathon detected that it was the target of a cybersecurity attack. An unauthorized third party attempted to infiltrate Parathon’s computer network and demand a ransom payment. Upon detecting this incident, we moved quickly to secure our network environment and launched a thorough investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to our systems and any personal information.

Although we have found no evidence that your information has been specifically accessed for misuse, it is possible that your name, address, date of birth, and/or protected health information, including but not limited to diagnosis, claims information, and health insurance information, to the extent that such may have existed on the network, could have been exposed. Notably, the types of information affected were different for each individual, and not every individual had all of the elements listed above exposed. **Importantly, the potentially exposed information does *not* include passwords, financial account information such as bank account numbers or credit card numbers, or social security numbers.**

As of this writing, Parathon has not received any reports of related identity theft since the date of the incident (July 27, 2023 to present). We have taken all efforts possible to mitigate any further exposure of your personal information and related identity theft.

What We Are Doing:

Data security is among Parathon’s highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Given this, we have taken and are continuing to take steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures to better protect the privacy and security of

information in our systems. We have also reviewed and taken steps to enhance our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

Additionally, while we have no evidence that your information has or will be misused, we are providing you with access to three different services offered services at no charge:

- Single Bureau Credit Monitoring
- Single Bureau Credit Report
- Single Bureau Credit Score

These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/parathon> and follow the instructions provided. When prompted please provide the following unique code to receive services: **W423U55PSL**.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Please keep this letter, as you will need to reference the enrollment code above when calling or enrolling online.

For More Information:

We encourage you to take full advantage of these services. Enclosed you will find additional materials regarding the resources available to you, and the steps you can take to further protect your personal information.

Cyberscout representatives are aware of the incident at Parathon and can answer questions or concerns you may have regarding protection of your personal information. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays. Please call the help line 1-833-929-2201 and supply the fraud specialist with your unique code listed above.

We value the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

James Dudley

James Dudley
President
Parathon by JDA eHealth Systems

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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; and
- (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are listed above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you

will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

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

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 1 Rhode Island residents that may be impacted by this event.