Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>:

Marathon Health provides on-site, near-site, and virtual health care to employees (and their family members) of various organizations. Marathon recently experienced an incident that involved personal information we maintain in one of our back-end health care operations databases. Unfortunately, we recently determined that your information may have been viewed or taken by an unauthorized person. This letter explains what happened, what information was involved, and what you can do to help protect that information.

What happened? On August 24, 2026, we received an alert of suspicious activity related to one of our employee's accounts. We immediately disabled the employee's account and began an investigation with the assistance of cybersecurity professionals. The investigation determined that an unauthorized individual posing as a Marathon IT worker was able to obtain the employee's credentials, used those credentials to access a cloud-hosted application, and exported information during that access. This all occurred within a few hours on August 24, 2026. We quickly began assessing the information potentially in scope and, on September 9, 2026, validated that personal information was obtained by the unauthorized person.

What data was involved? The information that may have been involved varied by individual. It may have included your name, date of birth, contact information, and Social Security number.

What we are doing. We wanted to notify you of this incident and assure you we take this matter very seriously. We arranged for you to receive a complimentary, <<12/24>>-month membership of identity monitoring services through Epiq Monitoring Solutions. This product includes credit monitoring, fraud consultation, and identity theft restoration. These services are completely free to you and enrolling in these services will not hurt your credit score.

To help prevent a similar incident from occurring in the future, Marathon Health has implemented, and will continue to adopt, additional safeguards to protect and monitor its environment.

What you can do. While we do not have evidence that your information was or will be misused, it is always a good idea to review financial-related statements you receive. If you see activity you do not recognize, please contact the issuing entity immediately. For more information on identity theft prevention, including additional steps you can take in response to this incident and instructions on how to activate your complimentary, <<12/24>>-month membership, please see the pages that follow this letter.

For more information. If you have questions, please call 888-517-6416 Monday through Friday, 9:00 AM to 9:00 PM Eastern Time, excluding holidays.

Sincerely,

Marathon Health