

Notice of Data Incident

We have become aware of a data incident that may have affected the privacy of certain information provided to us.

On February 28, 2026, we were alerted to unusual activity on its computer network and immediately began an investigation with the assistance of third-party specialists. The investigation determined that certain files on our network were accessed without authorization for a limited period of time from February 27 to February 28, 2026. We are currently conducting a comprehensive review and analysis of the files at issue to determine the types of information they contain and to whom the information relates. While this review remains ongoing, we believe a limited amount of protected health information (“PHI”) may have been subject to unauthorized access in connection with this event. At this time, we believe the information potentially at risk will vary by individual but may contain individuals’ first and last name in combination with one or more of the following: Social Security number, driver’s license number/government-issued ID number, date of birth, passport number, financial account information, diagnosis and treatment information, prescription information, provider name and location, dates of service, medical record number, patient account number, Medicare/Medicaid ID number, lab results, and/or health insurance information. Should our investigation identify potential impact to individuals’ information in relation to this incident, we will directly notify those individuals whose information is identified to have been at risk in accordance with applicable law. Because we took steps to ensure that the impacted data was re-secured and not distributed, we are not aware of any fraud or unauthorized publication of data resulting from this incident, nor do we have any reason to believe any such misuse of information will occur.

In response to this incident, we took immediate steps to secure our systems and engage third-party specialists to assist in a thorough investigation and response. Additionally, we have implemented additional security measures to further minimize the risk of a similar incident occurring in the future. We also notified law enforcement and are reviewing our policies and procedures related to data protection.

If you have any questions or would like to enroll in credit monitoring, please call 1- 833-931-3733 toll-free Monday through Friday from 8 A.M. to 8 P.M Central Time and please provide engagement reference number B175056. You may also write to us at 7880 Mission Grove, Parkway South, Riverside, CA 92508.

In general, we encourage individuals to remain vigilant in regularly reviewing and monitoring all account statements, explanation of benefits statements, and credit history to guard against any unauthorized transactions or activity. You may also place a fraud alert or credit freeze by contacting the credit reporting agencies: TransUnion 1-800-680-7289; Experian 1-888-397-3742; Equifax 1-888-298-0045. You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and steps to protect their personal information by contacting the credit reporting bureaus, the Federal Trade Commission (“FTC”), or their state Attorney General. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should also be reported to law enforcement, the state Attorney General, and the FTC.