

Berkeley Research Group Incident: Frequently Asked Questions

Express Scripts, UT System's pharmacy benefit manager, advised that some members will receive a notice from one of its vendors, Berkeley Research Group (BRG), regarding a data incident. Because the notice coming from BRG will reference neither UT System nor Express Scripts, the Office of Employee Benefits created this FAQ document to help contextualize the information members receive.

Q: What happened?

A: In November 2025, BRG reported that unauthorized parties accessed and/or acquired files containing information pertaining to Express Scripts' members. BRG reports it is unaware of any fraud or identity theft stemming from the incident.

Q: Who is Berkeley Research Group?

A: Berkeley Research Group (BRG) is a vendor used by Express Scripts for data consulting related to litigation. BRG is a global consulting firm that provides consulting, advisory, and expert witness services to clients and law firms, often in relation to ongoing litigation.

Q: How does this affect Express Scripts systems?

A: The unusual activity was isolated to BRG's systems and did not impact or threaten any Express Scripts systems. As of the date of this communication, Express Scripts advised it has no evidence that data has been misused but encourages vigilance as a precaution.

Q: What information was involved in this incident?

A: BRG reports the information involved varies by individual and may include some or all of the following: name, contact information, date of birth, social security number, health plan name, health insurance member ID, group member, member identification, medical record number, clinical or treatment information, prescription information, and payment history.

Q: Who is impacted?

A: Based on information provided by BRG, about 2,200 UT members were affected.

Q: Will affected individuals be notified?

A: BRG will notify impacted individuals and regulators. These notifications will be on behalf of BRG, and not Express Scripts. BRG will offer credit monitoring services to impacted members where applicable based upon the type of data impacted, such as social security numbers.

Q: When will affected individuals be notified?

A: Express Scripts advised it expects BRG to send notification near the end of April 2026.

Q: When was this suspicious activity identified?

A: According to Express Scripts, BRG provided preliminary notice on March 6, 2025 of unusual activity in its systems that occurred between February 28 and March 2, 2025.

Q: Why did it take so long to report unauthorized access?

A: According to Express Scripts, upon detecting suspicious activity, BRG took containment actions by taking systems offline and hired a third-party forensics firm to perform an investigation. Express Scripts advised the investigation, data mapping analysis, and validation were not completed until November 2025.

Q: How does Express Scripts assess BRG operations and security measures?

A: In accordance with supplier management processes, Express Scripts advised it performs security assessments of BRG. This includes an extensive industry standard security questionnaire, penetration testing, and independent third-party audit validation. To date, all findings have been addressed by BRG in a timely manner. Additionally, as part of the active monitoring of BRG's operations, Express Scripts regularly observes third party security ratings via Security Scorecard, which remain above industry average. Ongoing engagement continues to ensure transparency and oversight of BRG's cybersecurity practices.

Q: What should members do now?

A: Review the notice from BRG carefully, consider enrolling in any credit monitoring services offered, and remain vigilant by monitoring financial and healthcare-related accounts for suspicious activity.