BlueCross BlueShield of New Mexico

Conduent Cybersecurity Incident Frequently Asked Questions

Blue Cross and Blue Shield of New Mexico is sharing responses to the key questions we've seen from groups. If you have questions that aren't addressed below, please reach out to your account executive.

Q: Who is Conduent?
A: Conduent Inc. is a third-party services provider that offers printing/mailroom, document processing, payment integrity, government benefits and other back-office support services. Conduent had access to personal information due to the services it provides to its clients. BCBSNM has a Business Associate Agreement with Conduent.

Q: What happened?
A: According to Conduent, on Jan. 13, 2025, it discovered that they were the victim of a cyber incident that impacted a limited portion of their network. According to Conduent, they immediately secured their networks and initiated an investigation with the assistance of third-party forensic experts. Their investigation determined that an unauthorized third-party accessed their environment which included some files associated with BCBSNM.

Q: Were BCBSNM systems impacted by this incident?
A: No. BCBSNM systems were not impacted by this incident.

Q: How did you identify the suspicious activity?
A: On Jan. 17, 2025, Conduent Inc. notified BCBSNM that a threat actor had gained unauthorized access to their environment between Oct. 21, 2024, and Jan. 13, 2025.

NEW: Q: Please provide more information on how the threat actor gained access to Conduent's system.
A: According to Conduent, initial access to their environment was via a compromised account. All files sent to and from Conduent are encrypted in transit.

UPDATE: Q: Is there any way to tell what exact data elements were breached for each specific member?
A: Conduent has not provided BCBSNM with specific data elements for each member. However, according to Conduent, member notification letters will include member-specific data elements that were potentially disclosed. According to the information we received from Conduent, member information that was potentially disclosed includes: Name, Date of Birth, Postal Address Information, Social Security Numbers, medical service information (treatment and diagnosis codes, provider names, dates of service and claim amounts), group number and subscriber number.

Q: What is the plan for regulator, OCR, media, substitute, member or impacted individuals' notifications?
A: We continue to work through finalizing the notification processes with Conduent. Due to the scope and nature of the incident, which we understand impacts other entities, we plan to primarily delegate the individual notices to Conduent:

- Conduent will provide the OCR, substitute, attorney general and media notifications, and the notification letters to impacted members. We will provide the department of insurance notifications.
- We are working with Conduent to determine the timeline for the mailing of the member notification letters. Impacted individuals will be offered one year of free credit monitoring, unless a longer time frame (such as 18-24 months) is required under state law or otherwise required. The monitoring enrollment process will be detailed in the member notification letter.
- Conduent will have a call center available to address member questions once member notifications begin mailing. The number will be provided in the member notice.
- Conduent will post a substitute notification on its website and provide a media notice for the appropriate areas. We will link to the substitute notice from our websites once it is posted.

NEW: Q: How is Conduent/BCBSNM handling the media notices?
A: Conduent will provide media notices in the appropriate areas and jurisdictions.

NEW: Q: How will notifications be made to individuals?
A: Letters will be addressed to the specific member impacted, including minors. Kroll will offer minor specific identity theft protection services.

Q: Was data downloaded from Conduent's systems or was it only able to be viewed?
A: According to Conduent, the threat actors were able to exfiltrate the data.

Q: How many people were affected by the incident?
A: BCBSNM does not have information about total individuals or entities impacted by the Conduent incident. According to Conduent, they are not at liberty to discuss any other individuals or entities who may have been affected by this incident.

Q: Is this the extent of the impacted data for the breach; are all investigations closed at this time?
A: At this point in time, we believe the data evaluation at BCBSNM is complete; other aspects of the investigation are ongoing.

Q: Why did it take so long to notify impacted groups?
A: While this incident happened earlier this year, the data analysis by Conduent took extensive time. In July, Conduent provided the raw data to us. Due to the way the data was compiled when provided to BCBSNM, we subsequently undertook an evaluation to determine and verify the identity of the impacted members and which groups the individuals belong to, which was a time-consuming process.

Q: What was the date of containment?
A: We received communications from Conduent that the incident was contained on Jan. 27, 2025, and there was no longer an active threat. Conduent also provided official attestation to us.

Q: What security steps did Conduent take to respond to their incident?
A: According to Conduent, upon detection of the incident, Conduent activated its cybersecurity response plan with the help of external cybersecurity experts to contain and remediate the incident. Conduent notified the FBI. According to Conduent, they immediately took systems offline and retained cybersecurity experts to analyze their environment; Conduent later confirmed there has been no further known malicious activity since the event. All known indicators of compromise have been blocked. Conduent restored its systems and operations and implemented measures to further harden its systems.

Q: Are there any likely adverse effects of the data compromise on the impacted individuals?
A: At this point in time, Conduent states that it is not aware of actual or attempted misuse of the personal information. The member notification letter includes information on credit monitoring and steps members can take to help protect their information.

Q: Has Conduent communicated whether any evidence has been detected of the breached data appearing in known bad actor sites, forums, or on publicly accessible websites?
A: According to Conduent throughout this incident and investigation it has engaged in dark web monitoring for the disclosure of any data associated with this cyber incident being publicly released on the internet (including the dark web). To date, the results have been negative.

NEW: Q: Is BCBSNM pursuing any remedies with Conduent as a result of the breach, including terminating business with the vendor?
A: This is unknown at this time as our investigation and evaluation of the incident is ongoing.