

HUMANA INC
PRIVACY OFFICE
101 E MAIN STREET
LOUISVILLE KY 40202

RECEIVED

JUL 30 2026

CONSUMER PROTECTION
DIVISION

Humana

July 30, 2026

Office of the Attorney General
700 W. Jefferson Street, Suite 210
P.O. Box 83720
Boise, Idaho 83720-0010

RE: Case # 1277144

NOTICE OF DATA BREACH

Dear Attorney General,

The purpose of this letter is to notify your department of a recent security incident, pursuant to our Business Associate agreement, that occurred impacting 26 Humana members that reside in your State. First, let me state that Humana takes all privacy concerns seriously and is taking appropriate steps to prevent errors such as this in the future.

DentaQuest, LLC ("DentaQuest"), a dental and vision benefits provider for certain current and former Humana Medicaid and Dual Eligible Special Needs (D-SNP) plans. DentaQuest became aware of an unauthorized third party ("Threat Actor") claiming to be in possession of data allegedly originating from its IT environment on May 20, 2026. Humana learned that residents of your State were impacted by this incident on July 20, 2026.

What Happened?

The DentaQuest business, IT, and legal teams evaluated the situation and then engaged outside legal counsel and then retained CrowdStrike Services ("CrowdStrike") to conduct an independent investigation to assess the nature, scope, and extent of Threat Actor activity within the DentaQuest environment.

CrowdStrike confirmed unauthorized access to the DentaQuest environment occurred as a result of a social engineering attack targeting a single employee account. CrowdStrike's investigation has identified that the earliest evidence of Threat Actor activity in the DentaQuest environment occurred on May 17, 2026. At that time, the Threat Actor authenticated to DentaQuest's single sign-on (SSO) environment using credentials associated with the Impacted Account, with multifactor authentication (MFA) requirements satisfied through means consistent with the social engineering attack. CrowdStrike has not identified evidence of malware or ransomware deployment, privilege escalation, or additional persistence mechanisms established within the DentaQuest environment during the period of Threat Actor activity.

CrowdStrike has not identified evidence of Threat Actor access to the DentaQuest environment since May 19, 2026. DentaQuest implemented containment measures on May 20, 2026, and monitoring of the DentaQuest environment since that date has not identified evidence of further Threat Actor activity.

What Information Was Involved?

The data is known to include the following personal and dental or vision health information: name, address, member identification number, Medicaid number, Medicare number and dental or vision health information, including provider name, diagnosis treatment and billing information. In some instances, Social Security Number was included.

What We Are Doing

DentaQuest takes this incident and the security of information within their care very seriously.

DentaQuest immediately engaged legal counsel and launched an in-depth investigation upon discovery of this incident to determine the full nature and scope. The following measures were completed:

- Revoked all SSO sessions associated with the Impacted Account.
- Deactivated the Impacted Account and rotated associated credentials.
- Disabled application-specific access associated with the Impacted Account.

Notification letters are being sent to 26 residents of your State who were impacted by this situation. Attached you will find a copy of the letter that includes an application for free credit monitoring, and free identity theft protection by Kroll. Humana and/ or DentaQuest have also notified any applicable consumer reporting agencies and any other required agency.

DentaQuest encouraged individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports for suspicious activity and to detect errors. The notification letter included Kroll Identity Monitoring, Fraud Consultation and Identity Theft Restoration. It provided additional details on how to take steps to protect information, should an individual feel it is necessary to do so.

Humana will promptly report to your office and appropriate law enforcement officials any information that is shared with us that indicates this information has been inappropriately used.

Please do not hesitate to contact me if you have any additional questions regarding this situation.

Sincerely,

Privacy Office
Humana Inc.
privacyoffice@humana.com

Attachments