



Applies To: All Commercial Markets

Some Horizon Members Impacted by NASCO Cybersecurity Incident

NASCO, a provider of benefits administration services to health plans, including Horizon, has notified us of a cybersecurity incident.

What Happened?

NASCO was among the more than 1,000 entities worldwide that was impacted by the widely reported 2023 MoveIT cybersecurity incident. While this global cybersecurity incident affected more than 60 million individuals, our impact was limited to fewer than 5,000 of our members. Upon discovery of the cybersecurity incident, NASCO took appropriate steps to respond and prevent further illegal access.

What is Horizon Doing?

On **August 16, 2023**, Horizon received notice that some of its members were impacted by NASCO's cybersecurity incident. NASCO's leadership, forensics and legal teams continue to work with affected entities to assist with notification of the incident in accordance with applicable federal and state law.

We are sorry to report that this incident occurred, but rest assured we are working closely with NASCO to mitigate the risks associated with this incident.

What is NASCO Doing?

On or about **October 20, 2023**, [NASCO will mail letters](#) to affected plan members notifying them of this incident and offering them the option to accept free identity monitoring services. NASCO has arranged for Experian, a global leader in risk mitigation and response, to provide complimentary identity monitoring services for 24 months to impacted members. Experian will be establishing a dedicated assistance line for affected members to be published in the member letter to be sent by NASCO.

Additionally, NASCO will post media notices where required, notify the state Attorneys General in affected states as required by state law, and notify the Secretary of the U.S. Department of Health and Human Services (HHS) as required under federal law.

Protecting the privacy and security of our members' information is among our highest

priorities. We follow rigorous, industry-leading information security best-practices and we hold the vendors who assist Horizon in administering member benefits to the same standards. We will continue to work with NASCO to evaluate opportunities for improvements for data retention and disposition across environments.

If you have questions, please contact your sales executive or account manager.



Horizon Blue Cross Blue Shield of New Jersey will never send you an email asking you to click on a link to validate User ID(s), password(s) or PIN(s), Social Security Number(s), card or account number(s), cardholder verification value(s) (CVV2), or user-defined challenge information (e.g., mother's maiden name, place of birth, etc.). If such a message is received, please immediately forward it to Abuse@HorizonBlue.com.

Horizon Blue Cross Blue Shield of New Jersey is an independent licensee of the Blue Cross Blue Shield Association. The Blue Cross® and Blue Shield® names are registered marks of the Blue Cross Blue Shield Association. The Horizon® name and symbols are registered marks of Horizon Blue Cross Blue Shield of New Jersey.

© 2023 Horizon Blue Cross Blue Shield of New Jersey, Three Penn Plaza East, Newark, New Jersey 07105.

This email was sent from an unmonitored mailbox. If you have questions or prefer not to receive emails like this one from us in the future, please contact your Horizon sales executive or account manager.

ECN0010429

[View in browser.](#)