Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
[IDX URL]

Date: June [], 2026

<< Heading>>

Dear [],

We recently informed you about a vishing incident at CNO, and are now writing to follow-up on that incident. We take the privacy and security of your information seriously. Out of an abundance of caution, we are providing additional information to associates whose information may have been involved. We want you to be aware of the situation and to take advantage of the protective resources we are making available to you at no cost.

What Happened

On May 15, 2026, we were made aware of reports of fraudulent IT Service Desk calls targeting associates. This form of social engineering, known as "vishing," is where scammers use phone calls or voice messages to impersonate trusted organizations or internal departments.

We determined that a caller had attempted to gain unauthorized access to company data by contacting a small number of associates. Most of our associates were able to identify the scammer, ignore such calls, or escalate them appropriately. However, in one instance the scammer was able to gain limited unauthorized access.

When we first discovered this incident, we worked quickly, but with care, to fully understand its scope and impact. We engaged a leading security and forensics company to conduct an investigation into the matter, and we also reported this incident to U.S. federal law enforcement. Our investigation has shown no evidence to suggest that customer information was accessed, and customer service and other business operations were not disrupted.

<<state supplement.>>

What Information Was Involved

While the associate involved in this incident had, as part of their job responsibilities, access to certain employment-related data, we do not believe the scammer's goal was to target any of your personal information or intended to harm individuals. Instead, the evidence suggests that the scammer was motivated to target CNO and its company information, as is common with these types of incidents.

Nonetheless, we are providing you with this notice out of an abundance of caution because some of your personal information was involved. We believe that the limited amount of data that was involved included your <<PII list>>.

What We Are Doing

In response to this incident, we immediately launched an investigation into the scope and nature of the event. We are taking steps to further restrict access and enhance monitoring of internal systems, changing helpdesk procedures, and are investigating other protections to prevent further unauthorized activity. Lastly, we have raised awareness amongst associates regarding the risks of vishing and other social engineering attempts.

The investigation has not revealed any misuse of your information, or any attempts at fraud or identity theft. Out of an abundance of caution, we have engaged IDX, a leading identity protection services provider, to provide you with identity protection services at no cost. The complimentary services will be provided for a period of <<12/24>> months. IDX identity protection services include credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Please see the enclosed attachment for more information on credit monitoring and other steps you can take to protect your identity.

What You Can Do

To make the process as fast and simple as possible, *we have already enrolled you* in the IDX identity protection program. Please note, however, that *you must complete the credit monitoring services activation process yourself, as we are not permitted to activate those on your behalf*.

We encourage you to contact IDX with any questions about activating your free credit monitoring services by calling 1-xxx-xxx-xxxx. IDX representatives are available Monday to Friday, 9:00 AM to 9:00 PM Eastern Time.

As always, we encourage you to remain vigilant and to regularly monitor your account statements, financial transactions, and credit reports for any unusual or unauthorized activity, and to promptly report any concerns.

For More Information

We take privacy seriously and regret any inconvenience this incident may have caused you. We understand that receiving a notice like this can be concerning. Please know that we are committed to supporting you through this process and to taking every appropriate step to safeguard your personal information.

If you have any further questions or need more information, please see the *Recommended Steps to Help Protect Your Information* on the next page. You may also contact IDX by calling 1-xxx-xxx-xxxx if you have additional questions about this incident or if you need assistance in activating the IDX services.

Sincerely,

CNO Services, LLC

Recommended Steps to Help Protect Your Information

1. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

2. Telephone. Contact IDX at 1-xxx-xxx-xxxx to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop, and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting 1-866-349-5191 P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Reporting 1-888-397-3742 P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Reporting 1-800-680-7289 P.O. Box 2000 Chester, PA 19016-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to provide your personal information to place a freeze, and you will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia: Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, oag.dc.gov, Telephone: 1-202-727-3400.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, https://www.marylandattorneygeneral.gov, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.