NASCO

[*Experian Return Address Line 1*]
[*Experian Return Address Line 2*]

[*first_name*] [*last_name*]
[*address_1*]
[*address_2*]
[*city*], [*state_province*] [*postal_code*]

[*Letter_Date*]

Dear [*Full_Name*]:

NASCO, (collectively, "NASCO" or "we"), provides benefits administration services to health plan customers, including [insert]. We place a high value on maintaining the privacy and security of the information we maintain for our health plan customers. Regrettably, this letter is to inform you that a file sharing application we used to exchange files with your health plan was recently the victim of a cybersecurity attack, which impacted some of your personal information. This letter explains the incident, the measures we have taken in response and the steps you can take.

What Happened?
NASCO used a third-party software application, MOVEit Transfer by Progress Software ("MOVEit"), to exchange files. On May 30, 2023, NASCO experienced a data security incident in which a threat actor acquired data from NASCO's MOVEit instance. When NASCO learned of this incident on July 12, 2023, it promptly took steps to secure its systems, launched an investigation with the support of a leading cybersecurity firm and notified law enforcement authorities. Unfortunately, some personal information, including that of [insert] members, was involved.

As part of our investigation, NASCO analyzed the impacted data to determine whether any individual's personal information was subject to unauthorized access or acquisition. On [insert date], your health plan confirmed that, unfortunately, some of your personal information was affected by the incident.

What Information Was Involved? The personal information involved included your [*data_elements*]. We have no evidence that the personal information has been exploited to commit fraud.

What Are We Doing? We take the protection of your personal information seriously as data privacy and security are among our highest priorities, and we have extensive measures in place to protect information entrusted to us. Upon discovering the incident, we promptly took steps to mitigate the risk to our customers and personal information. The NASCO MOVEit server affected by the attack was decommissioned and is no longer accessible from the internet. MOVEit is no longer used by NASCO. Forensic evidence showed no threat actor activity outside of the MOVEit vulnerability exploitation. NASCO continues to work with law enforcement on this issue. To help prevent similar incidents from happening in the future, we have implemented and are continuing to implement additional procedures to further strengthen the security of our IT system environments.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports for suspicious activity and to detect errors. You should also review benefits documents that you receive from your heath plan to confirm that you received the health care services described. Enclosed with this letter are some steps you can take to protect your information.

As a measure of added security and to help protect your identity, we are offering a complimentary 24-month membership to Experian's® IdentityWorks℠. This product provides you with credit monitoring, identity theft resolution services, and $1,000,000 of identity theft insurance. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: [enrollment end date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [*URL*]
- Provide your **activation code**: [*code*]

NASCO

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [*customer service number*] by [*enrollment end date*]. Be prepared to provide engagement number [*engagement #*] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your personal information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [*customer service number*]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

For More Information. We regret that this incident occurred and any concern it may cause you. If you have additional questions, please call our dedicated, toll-free call center at 1-866-XXX-XXXX, Monday through Friday between 9:00 a.m. and 11:00 p.m. and Saturday and Sunday between 11:00 am and 8:00 pm Eastern Time, excluding major U.S. holidays.

Sincerely,

John Ladaga
President and CEO

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

NASCO

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com (800) 525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com (888) 397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com (800) 680-7289

Fraud Alerts. You may place a fraud alert on your file by calling one of the three nationwide credit reporting agencies above. 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.

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as indicated above.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and proof of current residential address (e.g., a copy of a utility bill, bank or insurance statement). Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates

must be recent). If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, the agency cannot charge you to place, lift or remove a security freeze. In all other cases, the credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze.

Report Incidents of Identity Theft. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should promptly report the issue to law enforcement, the FTC or your state Attorney General. For information on how to prevent or avoid identity theft, you can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

For North Carolina residents. For information on how to prevent identity theft, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.