NASCO MOVEIT PRIVACY INCIDENT

NASCO, a third-party provider of benefits administration services to health plans, 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, due to a previously unknown vulnerability in MOVEit, in which a threat actor acquired data from NASCO's MOVEit server. When NASCO learned of this incident on July 12, 2023, it promptly took steps to secure its systems, notified law enforcement authorities and launched an investigation that found that some of the acquired files contained the personal information of certain health plan members. NASCO is providing notification to impacted individuals and offering them 24 months of complimentary enrollment in Experian's identity monitoring services.

The information involved in the incident included the following data elements of some health plan members: [name, demographic information (including social security number, address, phone number, gender, date of birth), phone number, health insurance number, medical ID number, date of service, medical device or product purchased and provider/care giver name.] Importantly, not every affected individual had all of these data elements impacted, or the same combination of data elements impacted.

NASCO takes the protection of personal information seriously as data privacy and security are among our highest priorities. Upon discovering the incident, we promptly took steps to mitigate the risk to our customers and personal information. We encourage affected individuals to enroll in the complimentary identity monitoring services, to remain vigilant against incidents of identity theft and fraud, to review their account statements, and to monitor their free credit reports for suspicious activity and to detect errors. Affected individuals should also review benefits documents that they receive from their heath plan to confirm that you received the health care services described. The Reference Guide below describes some steps individuals can take to protect their information.

If you are an impacted health plan member with questions about the incident or how to enroll in Experian identity monitoring services, call 1-855-873-7643, 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.

We apologize for any inconvenience or concern this may cause. NASCO takes security very seriously and protecting your information is among our highest priorities. We have applied additional safeguards within our environment to further enhance threat prevention.

REFERENCE GUIDE

Affected individuals should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring credit reports for unauthorized activity.

Credit Reports. Under federal law, U.S. individuals are entitled to one free copy of their 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:

Table of credit reporting agencies

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 (as described below) 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.