Change Healthcare Notice of Data Security Incident Impacting Certain Participants of the National Automatic Sprinkler Industry Benefit Funds

Change Healthcare (CHC) is providing notice of a recent security incident which may affect the privacy of information of certain Participants of the National Automatic Sprinkler Industry Pension and Welfare Funds, and the National Automatic Sprinkler Metal Trades Pension and Welfare Funds (collectively, the "NASI Funds" or "NASI Benefit Funds"). CHC is a former vendor of the NASI Funds that provided administrative services.

CHC is providing this substitute notice to provide individuals with information about the cyberattack on CHC systems and to share information on steps individuals can take to protect their privacy, including enrolling in two years of complimentary credit monitoring and identity theft protection services if they believe their information may have been impacted. Affected individuals may also receive written correspondence from CHC regarding this incident.

What happened?

On February 21, 2024, CHC became aware of deployment of ransomware in its computer system. Once discovered, CHC quickly took steps to stop the activity, disconnected and turned off systems to prevent further impact, began an investigation, and contacted law enforcement.

CHC retained leading cybersecurity and data analysis experts to assist in the investigation, which began on February 21, 2024. On March 7, 2024, CHC confirmed that a substantial quantity of data had been exfiltrated between February 17, 2024, and February 20, 2024. On April 22, 2024, following analysis, CHC publicly confirmed the impacted data could cover a substantial proportion of people in America. Near the end of 2024, CHC notified the NASI Funds of the security incident and CHC identified approximately 7,441 NASI Fund participants whose data was affected.

What information was involved?

While CHC cannot confirm exactly what data has been affected for each impacted individual, CHC understands that impacted files involved participant's contact information (such as first and last name, address, date of birth, phone number, and email) and one or more of the following:

- Health insurance information (such as primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers);
- Health information (such as medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment);
- Billing, claims and payment information (such as claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due); and/or
- Other personal information such as Social Security numbers, driver's licenses or state ID numbers, or passport numbers.

CHC established a website and dedicated call center to offer additional resources and information related to this incident. You can visit changecybersupport.com or call the toll-free call center at: 1-866-262-5342, available Monday through Friday, 8 a.m. to 8 p.m. CT.

REFERENCE GUIDE

The NASI Funds encourage everyone to remain vigilant against incidents of identity theft and fraud. You should review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid, and monitor your credit reports for suspicious activity. Report any questionable charges or suspicious activity promptly to the provider or company with which you maintain the account.

Order your Free Credit Report

Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Upon receiving your credit report, review it carefully. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Enroll in IDX Credit and Identify Monitoring Services

At no cost, you may enroll in online credit monitoring and identity restoration services provided by IDX for two years. To enroll in these services, please call CHC at 1-866-262-5342 and ask to enroll.

Individuals must enroll in order for the available services to go into effect, and the monitoring included in the membership must be activated to be effective. Please note that credit monitoring services may not be available for individuals who have not established credit or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score. If you need assistance, IDX will be able to assist you.

Place a Fraud Alert on your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Request a Security Freeze on your Credit Report

For no cost, you have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian Security Freeze	**TransUnion**	**Equifax Security Freeze**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Current address and any previous addresses for the past five years;
5. Proof of current address, such as a current utility bill or insurance statement;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than 5 business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

Contact the U.S. Federal Trade Commission

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

If you believe you are the victim of a crime, you can contact local law enforcement authorities and file a police report.