On or about August 1, 2025, HSIP identified potential unauthorized access to its network. Once identified, HSIP took immediate steps to isolate and secure its network and engaged third-party specialists to assist with containing and investigating the activity. HSIP determined that certain data within its network was accessed and potentially copied without authorization. HSIP subsequently began reviewing the data to determine the contents of the data and to whom it related. HSIP completed their review on August 18, 2025 and identified that 13 Maine residents may have been affected by this event. The potentially impacted residents were associated with HSIP, and other data owners identified in the chart below.

Data Owner	***Population***
Teamsters Union 25 Health Services & Insurance Plan	6
Teamsters Local 25 Investment Plan	7

HSIP provided written notification to the potentially impacted Maine residents, on its behalf and on behalf of the data owners identified in the chart above, via First Class Mail on September 3, 2025, pursuant to Maine law. The notification letter includes details of the event and contact information for individuals to contact with inquiries. A copy of the notice letter is attached hereto as **Exhibit A**.

Exhibit A

[redacted]

Teamsters Union 25 Health Services & Insurance Plan
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

September 3, 2025

0000101102G0400

P

Dear [redacted]:

Teamsters Union 25 Health Services & Insurance Plan ("HSIP") writes to inform you of an event that may affect the privacy of your information. We are providing notice about the disclosure, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened. On August 1, 2025 we identified unauthorized activity within our network. Once identified, we took immediate steps to isolate and secure our network and engaged third-party specialists to assist with containing and investigating the activity. We have now determined that certain data within our network was accessed and potentially copied without authorization. We subsequently began reviewing the data to determine the contents of the data and to whom it related. We completed our review on August 18, 2025, and are now providing notification to potentially impacted individuals.

What Information Was Involved. The data that was potentially impacted varies by individual but may include your name and one or more of the following: [redacted].

What We Are Doing. Upon learning of this event, we immediately took steps to secure our network environment and undertook a thorough investigation. We are reviewing our policies and procedures, and implemented additional technical safeguards to further enhance the security of information in our possession and to prevent similar incidents from happening in the future. Additionally, we are offering you [redacted] months of complimentary credit monitoring and identity protection services.

What You Can Do. You can monitor your health records and insurance statements for any unfamiliar activity. Additionally, you should remain vigilant in regularly reviewing and monitoring all your account statements, explanation of benefits statements, and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources, including instructions on how to enroll in the complimentary credit monitoring services. Please note that you must enroll yourself into the credit monitoring services as we cannot enroll you on your behalf.

For More Information. If you have any questions, representatives are available for 90 days from the date of this letter, please call [redacted] Monday through Friday between 8:00 am and 8:00 pm. Eastern time, excluding holidays. You can also write to us at 529 Main Street, Suite 209, Charlestown, MA 02129.

Sincerely,

Teamsters Union 25 Health Services & Insurance Plan ("HSIP")

[redacted]

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Identity Monitoring Services

We are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation service

To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

[redacted]

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or www.ag.ny.gov.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 1-202-727-3400, and www.oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For 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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this matter. There are 106 Rhode Island residents impacted by this matter.

[redacted]