EXHIBIT 1

By providing this notice, North Atlantic States Carpenters Benefit Funds, consisting of the North Atlantic States Carpenters Pension Fund, the Guaranteed Annuity Fund, the Health Benefit Fund, the Annuity Fund and the Vacation Fund (collectively "NASCBF") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about August 18, 2025, the NASCBF observed suspicious activity within the network of the Hamden, CT office. The NASCBF promptly reset passwords, took measures to limit the impact of the incident, and started a forensic investigation with the assistance of third-party specialists. The investigation determined that an unauthorized actor accessed and/or acquired certain files on the systems of the CT office on August 18, 2025. The NASCBF then undertook a comprehensive review of the affected files to determine the full scope of any impacted individuals. This review was completed on January 13, 2026, and the NASCBF has been working to determine who was potentially impacted and confirm address information for those individuals. No funds were taken, and participants' benefits and account balances with the NASCBF are fully intact.

The information that could have been subject to unauthorized access includes name, Social Security number, and financial account information.

Notice to Maine Residents

On or about February 11, 2026, NASCBF provided written notice of this incident to two thousand sixty-three (2,063) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, NASCBF moved quickly to investigate and respond to the incident, assess the security of NASCBF systems, and identify potentially affected individuals. Further, NASCBF notified federal law enforcement regarding the event. NASCBF is currently reviewing the protocols, policies, and procedures to reduce the likelihood of a similar event occurring in the future. NASCBF is providing access to credit monitoring services for twelve (12) months, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, NASCBF is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. NASCBF is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

NASCBF is providing written notice of this incident to relevant state and federal regulators, as necessary. NASCBF is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

North Atlantic States
CARPENTERS BENEFIT FUNDS

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

<<VARIABLE DATA 1>>

Dear <<Full Name>>:

The North Atlantic States Carpenters <<Variable Data 2>>, collectively the North Atlantic States Carpenters Benefit Funds ("NASCBF"), is writing to inform you of a data event that may involve some of your personal information. Though we have no evidence of any actual or attempted identity theft or fraud in connection with this event, this letter provides you with information about what happened, our response to date, and steps you can take to help protect your personal information, should you feel it appropriate to do so. **We want to stress that no funds were taken, and participants' benefits and account balances with the NASCBF are fully intact.**

What Happened? On or about August 18, 2025, the NASCBF observed suspicious activity within the network of the Hamden, CT office. The NASCBF promptly reset passwords, took measures to limit the impact of the incident, and started a forensic investigation with the assistance of third-party specialists. The investigation determined that an unauthorized actor accessed and/or acquired certain files on the systems of the CT office on August 18, 2025. We then undertook a comprehensive review of the affected files to determine the full scope of any impacted individuals. Our review was completed on January 13, 2026, and the NASCBF has been working to determine who was potentially impacted and confirm address information for those individuals.

What Information Was Involved? The types of information that may have been impacted includes your name and the following: <<data elements>>.

What We Are Doing. Upon discovering the incident, the NASCBF promptly launched an investigation to determine what happened and what information may be involved. As part of the NASCBF's ongoing commitment to information security, it is currently reviewing the protocols, policies, and procedures to reduce the likelihood of a similar event occurring in the future. The NASCBF also notified law enforcement and will notify appropriate state and federal regulators, as required. Additionally, though we have no evidence of misuse of your information, we are offering credit monitoring for <<CM Duration>> months through Epiq at no cost to you. Instructions on how to enroll can be found in the enclosed *Steps You Can Take to Help Protect Your Personal Information.* Please note that you must enroll yourself in these services as we are unable to do so on your behalf due to privacy concerns.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. Information on how to obtain a free credit report, implement a credit freeze or fraud alert, how to enroll in the complimentary credit monitoring services, and other guidance can be found in the enclosed *Steps You Can Take to Help Protect Your Personal Information.*

For More Information. We understand that you may have questions that are not addressed in this letter. If you have additional questions, please call 855-720-3044 from Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. You may also write to us at 350 Fordham Road, Wilmington, MA 01887.

Sincerely,

The North Atlantic States Carpenters Benefit Funds

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Monitoring Services

<<Full Name>>
Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: <<CM Duration>> Months

Epiq - Privacy Solutions ID
1B Credit Monitoring - Plus

How To Enroll:

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

1-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score and Report[1]
1-Bureau VantageScore® 3.0 (annual) and 1-Bureau Credit Report.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)
Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring
Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection
Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance[2]
Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT[2]
Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Plus, please call directly at **866.675.2006,** Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. 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. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.

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 https://ag.ny.gov.

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 reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.