5/22/2026

[redacted]

NOTICE OF DATA BREACH

As you may know, the Metro-ILA Pension Fund, Metro-ILA Fringe Benefit Fund and Metro-ILA Individual Account Retirement Fund (the "**Funds**") provide your employee benefits pursuant to collective bargaining agreements between the Metropolitan Marine Maintenance Contractors' Association (the "**MMMCA**") and the ILA. Both the Funds and the MMMCA respect the privacy of your information. We are writing to inform you that your personal information was included in a recent data breach of the Funds' and the MMMCA's data systems.

We recognize that this news can be unsettling to impacted members. We take your well-being and privacy very seriously, and want you to have all the information you need to respond appropriately. Finally, we want you to know what happened, what information was involved, what we did thus far, what else is being done in response to the incident, and what you can do to help protect yourself against possible misuse of the information.

What Happened

On or about April 7, 2026, the Funds and the MMMCA identified a cybersecurity incident involving unauthorized activity in their network environment. Upon discovery, the Funds and the MMMCA promptly, through legal counsel, engaged third-party forensic and data-mining experts to investigate the nature and scope of the incident and to determine what information was accessed or compromised. At this time, we believe that an unknown threat actor gained access to the Funds' and the MMMCA's environment by utilizing one of the Funds' and the MMMCA's virtual private networks ("**VPN**"). As of April 20, 2026, forensic experts have advised that there is no indication of a persistent threat with access to and within the Funds' and the MMMCA's environment. The investigation remains ongoing, and the Funds and the MMMCA are actively working to identify affected individuals and data elements.

What Information Was Involved

With the support of forensic and data mining experts, the Funds and the MMMCA have been working diligently to determine the impact of the threat actor's actions and individuals impacted by the attack. At this time, based on our internal investigation, we believe that the categories of your personally identifiable information impacted by this incident were **Social Security Number; Date of Birth; Phone Number; Address.**

What We Have Done and What We Are Doing

Prior to this breach, the Funds and the MMMCA maintained reasonable security measures, including without limitation, strong password protocols and two factor authentication. While the Funds and the MMMCA already had robust security measures in place prior to this breach, the Funds and the MMMCA have taken, and plan to take, additional measures to further harden their environment, including, without limitation, removal of the threat actor's point of entry, reset of all personnel passwords, enhancement of end point detection tools, and deployment of multifactor across all accounts, VPNs, and other devices and systems connected to the Funds' and the MMMCA's environment.

We have informed law enforcement of the incident. To date, we have not received any reports regarding any unauthorized use of personal information beyond the initial incident. **We are also offering you twelve (12) months of free credit monitoring services from Experian. Please see the Credit Monitoring Service Enrollment Information page at the**

METRO - I.L.A. FUNDS & MMMCA, Inc.
301 ROUTE 17N • 7TH FLOOR • RUTHERFORD, N.J. • 07070
TEL: 201 • 842 • 0202
Fax: 201 • 842 • 0334

end of this document for details on how to enroll. You will have until September 30, 2026 to sign up.

What You Can Do

We strongly recommend you (1) sign up for the Experian credit monitoring service as explained in the enclosed Experian information sheet at the end of this letter, (2) remain vigilant, monitor and review all your financial and personal account statements and credit reports, and (3) immediately report any unusual activity to the institution that issued the record and to law enforcement.

Should you receive a call, email, or other communication from someone who claims to have your personal information:

- Do not engage with the caller/correspondent, and do not offer details about the attack or what may have occurred.
- Listen carefully and immediately following the call, make notes about what you were told.
- As soon as possible, please share the information with us. We will make sure you receive the information you need to properly respond to the situation.
- In addition, you can reach out to local law enforcement or the respective state Attorney General. We also encourage you to contact local authorities to obtain a police report.

For your personal accounts and devices, we strongly recommend that you (i) change default passwords, (ii) use robust passwords and/or passcodes, and do not recycle passwords or use the same password across multiple accounts or devices, and (iii) wherever available on personal devices and accounts, implement two factor authentication.

Also enclosed with this notice is a resource sheet containing additional information for your general reference, listing toll-free numbers and addresses of the three largest nationwide consumer reporting agencies and Federal Trade Commission. This reference is provided in addition to the 12 months of Credit Monitoring Service if you choose to enroll.

For More Information

If you have any questions regarding this information, please contact us by email at [redacted] or by telephone at [redacted]

Respectfully,

MMMCA, Inc. & Metro-ILA Funds

ATTACHMENT

IF YOUR IDENTITY IS COMPROMISED STEPS YOU CAN TAKE:

- **Local Police Reporting**

File a report with your local police department.

- **Passwords, Passcodes**

Change passwords and passcodes on all personal accounts and devices. Often, people will use the same password that they use for one account or device for multiple accounts and/or devices. If you change passwords, this should include your personal social media accounts, online banking accounts, cellphones, tablets, home computers, etc. Best practice is not to use the same password for more than one account or device, nor to "recycle" or reuse passwords that were used in the last several years. If your accounts offer multi-factor authentication, we suggest you enable this for those accounts.

- **Social Security Administration**

Block Electronic Access: If you know your Social Security information has been compromised, you can request to Block Electronic Access. This is done by calling the Social Security Administration National 800 number (Toll Free 1-800-772-1213 or at our TTY number at 1-800-325-0778). Once requested, any automated telephone and electronic access to your Social Security record is blocked. Note: No one, including you, will be able to see or change your personal information on the internet or through the Social Security Administration's automated telephone service. If you have requested that the Social Security Administration block access to your record and later change your mind, you can contact the Social Security Administration and ask to have the block removed. You will need to prove your identity when you call the Social Security Administration. See also: https://www.ssa.gov/pubs/EN-05-10220.pdf.

- **IRS**

Complete IRS Form 14039. The form can be found at: https://www.irs.gov/newsroom/tips- for-taxpayers-victims-about-identity-theft-and-tax-returns-2014.You can contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

We encourage you to monitor your financial accounts, including the account you use for direct deposit, and ask your account manager for additional services or resources that your bank may offer to protect your accounts. Remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://consumer.ftc.gov/identity-theft-and-online-security To file with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Theft of your social security number should also be reported to the FTC at https://www.identitytheft.gov/.

- **Copy of Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report, general inquiries, placing a fraud alert on your credit

report, or requesting a credit freeze is provided below:

Experian	TransUnion	Equifax
1-888-EXPERIAN (397-3742)	1-800-680-7289	1-800-525-6285
P.O. Box 9532	Fraud Victim Assistance Division	P.O. Box 740241
Allen, TX 75013	PO Box 2000	Atlanta, GA 30374-0241
www.experian.com	Chester, PA 19016	www.equifax.com
	www.transunion.com	

- **Fraud Alert**

We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

- **Credit Freezes**

You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security 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 security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. 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. If you have moved in the past five years, provide the addresses where you have lived during such time
5. Proof of current address such as current utility bill or telephone bill
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 the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specific period of time.

To remove the security freeze, you must submit a request through a toll-free number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Additional resources may be available from your state. Please see the below listing for your state. Note that not all states have additional sites.

Alabama: The State of Alabama also offers a resource page on identity theft, which can be found at https://www.revenue.alabama.gov/faqs/if-i-am-a-victim-of-identity-theft-what-should-i-do/.

Arizona: Arizona's Attorney General Office provides additional information, which can be found at https://www.azag.gov/consumer/data-breach/identity-theft.

Arkansas: Arkansas's Attorney General Offices provides additional information, which can be found at https://arkansasag.gov/consumer-protection/identity/what-should-victims-do/.

California: The State of California also offers a resource page on identity theft, which can be found at https://oag.ca.gov/idtheft/facts/victim-checklist.

Colorado: The State of Colorado also offers a resource page on identity theft, which can be found at: https://stopfraudcolorado.gov/fraud-center/identity-theft.html.

Connecticut: The State of Connecticut also offers a resource page on identity theft, which can be found at https://portal.ct.gov/ag/consumer-issues/identity-theft/identity-theft.

District of Columbia (DC): The District of Columbia also offers resources on identity theft, which can be found at: https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft#:~:text=In%20the%20District%20of%20Columbia%2C%20the%20Financial%20and,telephone%20at%20202-727-4159.%20Via%20the%20Internet%20at%20https%3A%2F%2Fwww.mpdc.dc.gov

Florida: The State of Florida also offers a resource page on identity theft, which can be found at: https://www.fdacs.gov/Consumer-Resources/Scams-and-Fraud/Identity-Theft/Identity-Theft. For additional information, please call the Florida Attorney General's Identity Theft Victim Services toll-free telephone number at 1-866-9-NO-SCAM.

Georgia: The State of Georgia also offers a resource page on identity theft, which can be found at: https://consumer.georgia.gov/consumer-topics/identity-theft. See also https://dds.georgia.gov/georgia-licenseid/existing-licenseid/how-do-i-replace-license.

Idaho: https://tax.idaho.gov/guides/protecting-your-identity/identity-theft/

Illinois: Illinois also offers a resource page on identity theft, which can be found at: https://www.illinoisattorneygeneral.gov/consumers/hotline.html

Indiana: The State of Indiana also offers a resource page on identity theft, which can be found at: https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/complaint-form/

Iowa: https://www.iowaattorneygeneral.gov/for-crime-victims
Office of the Attorney General of Iowa
Victim Assistance Section
Hoover State Office Building
1305 East Walnut Street
Des Moines, IA 50319

Phone: 515-281-5044
Toll-Free: 800-373-5044
FAX: 515-281-8199

Kansas: Kansas provides the following resource page: https://www.ag.ks.gov/divisions/public-protection/your-identity#:~:text=Request%20a%20fraud%20alert&text=Equifax%3A%201%2D800%2D525,1%2D800%2D680%2D7289

Kentucky: The Commonwealth of Kentucky also offers a resource page on identity theft, which can be found at:

https://www.ag.ky.gov/Resources/Consumer-Resources/Consumers/Pages/Identity-Theft.aspx. See also https://drive.ky.gov/Drivers/Pages/Renew-Replace-Update.aspx.

Louisiana: The Commonwealth of Louisiana also offers a resource page on identity theft, which can be found at: https://revenue.louisiana.gov/FraudForms/IdentityTheftChecklist.pdf

Maryland: Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

Massachusetts: The State of Massachusetts also offers a resource page on identity theft, which can be found at: https://www.mass.gov/protecting-yourself-if-your-identity-is-stolen. For additional information, please call the Massachusetts Attorney General's Consumer Advocacy & Response Division, Consumer Hotline at (617) 727-8400.

Michigan: Michigan's Attorney General Office offers additional resources at https://www.michigan.gov/ag/initiatives/michigan-identity-theft-support.

Minnesota: The State of Minnesota also offers resource pages on identity theft, which can be found at: https://dps.mn.gov/divisions/ojp/help-for-crime-victims/Pages/Identity%20Theft.aspx and also https://www.revenue.state.mn.us/mndor-pp/6466?type=html

Mississippi: The State of Mississippi also offers a resource page on identity theft, which can be found at https://www.its.ms.gov/services/identity-theft.

Montana: Montana's Department of Justice provides further information at **https://dojmt.gov/consumer/identity-theft/**https://dojmt.gov/consumer/identity-theft/.

Nebraska: The Nebraska Attorney General provides an Identity Theft Consumer Guide which can be found at https://protectthegoodlife.nebraska.gov/sites/default/files/doc/Identity Theft June 2023.pdf.

Nevada: Nevada offers resources at https://ag.nv.gov/Hot_Topics/Victims/IDTheft_Victim_Information/.

New Hampshire: New Hampshire's Department of Justice offers a guide for victims of identity theft which can be found athttps://www.doj.nh.gov/citizens/consumer-protection-antitrust-bureau/identity-theft#:~:text=Call%20the%20FTC%27s%20toll%2Dfree,%2D888%2D468%2D4454.

New Jersey: The State of New Jersey also offers a resource page on identity theft, which can be found at https://www.cyber.nj.gov/guidance-and-best-practices/identity-theft-privacy/identity-theft-and-compromised-pii.

New Mexico: The New Mexico Department of Justice offers victim resources https://nmdoj.gov/about-the-office/criminal-affairs/#victim-services.

New York: The State of New York also offers a resource page on identity theft, which can be found at: https://ag.ny.gov/consumer-frauds-bureau/identity-theft.

North Carolina: North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or by contacting North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001. 877-566-7226 (Toll-free within North Carolina). 919-716-6000.

Ohio: The State of Ohio also offers a resource page on identity theft, which can be found at https://www.ohioattorneygeneral.gov/identitytheft#. For the Bureau of Motor Vehicles, see https://bmvonline.dps.ohio.gov/home/. For additional information, please visit https://www.ohioattorneygeneral.gov/FAQ/Responding-to-Identity-Theft-FAQs.

Oregon: Oregon provides the following resource page with Identity theft protection resources https://www.oregon.gov/dor/programs/individuals/pages/protecting-your-identity.aspx.

Oklahoma: The State of Oklahoma also offers a resource page on identity theft, which can be found at:

https://oklahoma.gov/okdhs/library/idresources.html.

Pennsylvania: The Commonwealth of Pennsylvania also offers a resource page on identity theft, which can be found at: https://www.attorneygeneral.gov/protect-yourself/identity-theft/.

Rhode Island: Rhode Island residents may request additional information by contacting: Rhode Island, Office of the Attorney General, 150 South Main Street**,** Providence, Rhode Island 02903. Tel: 401-274-4400. Rhode Island also offers a resource page on identity theft, which can be found at https://riag.ri.gov/what-we-do/civil-division/public-protection/consumer-protection/id-theft.

South Carolina: The State of South Carolina also offers a resource page on identity theft, which can be found at: https://consumer.sc.gov/identity-theft-unit/id-theft.

South Dakota: The State of South Dakota also offers a resource page on identity theft, which can be found at https://consumer.sd.gov/fastfacts/identitytheft.aspx.

Tennessee: The State of Tennessee also offers a resource page on identity theft, which can be found at: https://www.tn.gov/content/dam/tn/safety/documents/IdentityTheftVicrimToolkit.pdf.

Texas: The State of Texas also offers a resource page on identity theft, which can be found at https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/identity-theft-resources.

Utah: Utah offers additional information which can be found at: https://dcp.utah.gov/education/identity-theft/. The Utah State Tax Commission also provides resources at: https://tax.utah.gov/individuals/identity-theft.

Vermont: The State of Vermont also offers a resource page on identity theft, which can be found at https://ago.vermont.gov/cap.

Virginia: The Commonwealth of Virginia also offers a resource page on identity theft, which can be found at: https://www.oag.state.va.us/programs-outreach/identity-theft. See also: https://www.dmv.virginia.gov/licenses-ids/license/applying/identity-theft.

Washington: Washington State also offers additional information which can be found at: https://www.atg.wa.gov/recovering-identity-theft-or-fraud.

West Virginia: The State of West Virginia also offers a resource page on identity theft, which can be found at: https://ago.wv.gov/consumerprotection/Pages/Identity-Theft-Prevention.aspx.

Wisconsin: The State of Wisconsin also offers a resource page on identity theft, which can be found at: https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftResources.aspx.
See also: https://datcp.wi.gov/Documents/IDTheftWhatToDo602.pdf.

CREDIT MONITORING SERVICES
Enrollment Information
with Experian IdentityWorks

To help protect your identity, the Funds are offering a complimentary 12-month membership of Experian's® IdentityWorks[SM]. This product provides you with superior identity detection and resolution of identity theft. To activate your FREE 12 month membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **September 30, 2026, 11:59pm UTC.**
- (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/1bcredit/
- Provide your **activation code**: [redacted]

- **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 (**833) 931-7577 **by September 30, 2026, 11:59pm UTC.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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[TM]**: 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 information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 931-7577. 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 to you for 12 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.

* 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.