

Colin M. Battersby
Direct Dial: (248) 593-2952
E-mail: cbattersby@mcdonaldhopkins.com

October 24, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Northeast District Council of the OPCMIA Fringe Benefit Funds – Incident Notification

Dear Attorney General Frosh:

McDonald Hopkins PLC represents Northeast District Council of the OPCMIA Fringe Benefit Funds (“NEDC”). I am writing to provide notification of an incident at NEDC that may affect the security of personal information of ten (10) Maryland residents. By providing this notice, NEDC does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On March 8, 2023, NEDC learned an unauthorized individual obtained access to two NEDC employee email accounts. Upon learning of this issue, NEDC contained the threat and secured the email accounts, and immediately began a prompt and thorough investigation. As part of the investigation, NEDC worked very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and comprehensive review of all the data impacted, on September 12, 2023, NEDC discovered that the impacted email accounts contained individual personal information. The information potentially accessed include full name, Social Security number and health information. Due to the limited evidence available, NEDC was not able to definitively determine whether individual personal information was accessed and/or acquired by the unauthorized individual as a result of the incident, however, we wanted to notify you and the potentially affected residents of the incident out of an abundance of caution.

NEDC has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, NEDC wanted explain the steps that it is taking to help safeguard the affected residents against identity fraud. NEDC is providing the affected residents with written notification of this incident commencing on or about October 24, 2023 in substantially the same form as the letter attached hereto. NEDC is also offering the affected residents

October 24, 2023

Page 2

complimentary one-year membership with a credit monitoring service. NEDC will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. NEDC will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At NEDC, protecting the privacy of personal information is a top priority. NEDC is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. NEDC continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com.

Very truly yours,



Colin M. Battersby

Encl.



***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

October 24, 2023

Dear [REDACTED]

At Northeast District Council of the OPCMIA Fund ("NEDC"), we take the protection of your personal information very seriously. We are writing with important information regarding a network security incident NEDC has experienced. The privacy and security of the personal information we maintain is of the utmost importance to us. As such, we wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

An unauthorized individual obtained access to two NEDC employee email accounts between approximately January 12, 2023 and April 12, 2023.

What We Are Doing.

Upon learning of the incident, we commenced a prompt and thorough investigation. We immediately took steps to remediate the issue and to investigate any potential unauthorized access to the email environment. As part of our investigation, we have worked very closely with third party cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, on September 12, 2023, we discovered that the impacted email accounts contained your personal information. Due to the limited evidence available, we were not able to definitively determine whether your personal information was accessed and/or acquired by the unauthorized individual as a result of the incident. However, we wanted to notify you of the incident out of an abundance of caution and provide you with information on how to best protect your identity.

What Information Was Involved?

The impacted email accounts contained your first and last name, and Social Security number.

What You Can Do.

We have no evidence your information has been specifically misused, however to protect you from potential misuse of your information, we are offering you complementary credit monitoring services with Cyberscout, a TransUnion company. We are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. 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. For more information on identity theft prevention and the credit monitoring services, including instructions on how to activate your membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on any credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and monitoring your free credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apology that this incident occurred. We are committed to maintaining the privacy of your information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of the personal information in our possession, and have taken steps to further protect unauthorized access to individual records.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against misuse of your information. The response line is available Monday through Friday, 8:00 am to 8:00 pm Eastern Time, excluding holidays.

Sincerely,

Northeast District Council of the OPCMIA Fund

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring

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.

2. Placing a Fraud Alert

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069

Atlanta, GA 30348-5069

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

(800) 525-6285

Experian

P.O. Box 9554

Allen, TX 75013

<https://www.experian.com/fraud/center.html>

(888) 397-3742

TransUnion

Fraud Victim Assistance

Department

P.O. Box 2000

Chester, PA 19016-2000

<https://www.transunion.com/fraud-alerts>

(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(888)-298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.