



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

December 4, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Metropolitan Council located at 390 Robert Street N, St. Paul, Minnesota 55101, and write to notify your office of an event that may affect the security of certain personal information relating to approximately three (3) Maryland residents. This notice may be supplemented if significant new facts learned subsequent to its submission. By providing this notice, Metropolitan Council does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 12, 2024, Metropolitan Council identified suspicious activity in an employee's email account. Metropolitan Council promptly took steps to ensure the security of the email tenant and launched a comprehensive investigation, with the assistance of third-party cybersecurity and digital forensics specialists, into the nature and scope of the event. The investigation determined an unauthorized actor gained access to certain employee email accounts and an associated cloud storage platform for various periods of time between March 27, 2024 and May 27, 2024.

The investigation was unable to identify with specificity the full scope of emails or information were viewed by the unauthorized actor in the accounts. Out of an abundance of caution, Metropolitan Council is taking steps to notify all individuals whose information may have been contained within the accounts subject to access by the unauthorized actor.

The information that could have been subject to unauthorized access includes private benefit information, which may include an individual's name and Social Security number.

Notice to Maryland Residents

On or about November 13, 2024, Metropolitan Council began providing written notice of this event to potentially affected individuals. On December 3, 2024, Metropolitan Council continued provided notice of this event, including to three (3) Maryland residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon identifying the event, Metropolitan Council moved quickly to investigate and respond, secure Metropolitan Council's email tenant, identify potentially affected individuals, and issue notification. Metropolitan Council is also working to implement additional cybersecurity safeguards and training to its employees. Metropolitan Council is providing access to credit monitoring services for 1 year, through IDX, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, Metropolitan Council is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud. Metropolitan Council 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.

Metropolitan Council is providing written notice of this event to appropriate state privacy regulators, and to the three major consumer reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/jlm
Enclosure

EXHIBIT A



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

December 3, 2024

Notice of <<Data Breach/Security Incident>>

Dear <<First Name>> <<Last Name>>:

Metropolitan Council's Housing and Redevelopment Authority ("Metro HRA") writes to inform you of an event relating to the confidentiality of certain information in our care. While there is no evidence of actual or attempted misuse of information as a result of this event, in an abundance of caution, we are providing you with an overview of the event, our response, and additional resources to help further protect your information, should you feel it is appropriate to do so.

What Happened? On or about April 12, 2024, Metro HRA identified suspicious activity in an employee's email account. We promptly took steps to ensure the security of the email tenant and launched a comprehensive investigation, with the assistance of cybersecurity specialists, into the nature and scope of the event. The investigation determined an unauthorized actor gained access to certain employee email accounts for various periods of time between March 27, 2024 and May 27, 2024.

As part of the investigation, we undertook a review of the data within the impacted accounts to determine what information may be involved and to whom the information relates. This review concluded recently and determined that some of your information may be involved.

What Information Was Involved? The review identified that there was access to some SharePoint documents and some Metropolitan Council emails. It is possible that private benefit data about you was viewed, potentially including your name, address, phone number, and social security number. Please note, there is no evidence of actual or attempted identify theft or fraud associated with this event.

What We Are Doing. We take this event and the privacy of the information in our care very seriously. Upon learning of the event, we moved quickly to assess the security of the email system and investigate the event. We are also reporting this event to appropriate regulators. As part of our commitment to information security, we are reviewing our policies, procedures, and training protocol to reduce the risk of a similar events from occurring in the future. Metropolitan Council is also preparing a summary of the event and our investigation. Should you wish to obtain this summary, please contact our dedicated assistance line at the phone number below. You will be asked to provide your name and contact information so that Metropolitan Council can provide you the summary via email or mail.

We are also offering <<12/24>> months of complimentary credit monitoring through IDX. You must enroll in these services yourself as we cannot do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Information*, which includes further information and resources. Additionally, we encourage you to enroll in the complimentary credit monitoring being offered.

For More Information. If you have additional questions, please contact our toll-free assistance line at 1-877-718-6103. IDX representatives are available Monday through Friday from 9:00 am – 9:00 pm Eastern Time, excluding U.S. holidays. Please note the deadline to enroll is March 3, 2025. You may also write to the Metro HRA at 390 Robert Street North, St. Paul, MN 55101.

Sincerely,

Ryan O'Connor
Regional Administrator

STEPS YOU CAN TAKE TO HELP PROTECT INFORMATION

Enroll in Monitoring Services

Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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 one-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/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, 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. Fees may be required to be paid to the consumer reporting agencies. There are approximately 0 Rhode Island residents that may be impacted by this event.