

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

March 21, 2024

VIA U.S. MAIL

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



Re: City of Conneaut – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents the City of Conneaut. I am writing to provide notification of an incident at City of Conneaut that may affect the security of personal information of approximately one (1) Maryland resident. By providing this notice, City of Conneaut does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

City of Conneaut discovered unauthorized access to a single email account on or about December 15, 2023. Upon learning of this issue, City of Conneaut immediately took steps to secure the email account and commenced a prompt and thorough investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of incidents.

Based on its comprehensive investigation and manual document review, which concluded on February 22, 2024, City of Conneaut discovered that certain documents in the email account contained personal information and was potentially accessed and/or acquired by an unauthorized actor. The impacted files contained the personal information of certain individuals, including the identified resident's full name, address, date of birth, medical treatment information, health insurance information, provider, and/or diagnosis information.

To date, City of Conneaut is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, City of Conneaut wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. City of Conneaut is providing the affected resident with written notification of this incident commencing on or about March 21, 2024 in substantially the same form as the letter attached hereto. City of Conneaut is advising the affected resident about the process for placing fraud alerts and/or security freezes 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

Baltimore | Chicago | Cleveland | Columbus | Detroit | West Palm Beach

mcdonaldhopkins.com

Page 2

Commission. The affected resident is also being provided steps to take to safeguard themselves against medical identity theft.

At City of Conneaut, protecting the privacy of personal information is a top priority. City of Conneaut is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. City of Conneaut continues to evaluate and improve, where appropriate, its administrative and technical safeguards including training its employees on best practices related to cybersecurity, policies, procedures, and protocols, and tools to protect its network environment.

Should you have any questions concerning this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'D. Paluzzi', with a stylized flourish at the end.

Dominic A. Paluzzi

Encl.

City of Conneaut, Ohio

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]



[REDACTED]
[REDACTED]
[REDACTED]

March 21, 2024

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]

The privacy and security of the personal information entrusted to us is of the utmost importance to the City of Conneaut. ("Conneaut"). We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved some of your personal information. 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?

On or about December 15, 2023, City of Conneaut detected unauthorized access to a single email account.

What We Are Doing.

Upon learning of this issue, City of Conneaut immediately took steps to secure the email account and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Following this investigation and our manual review, we learned on February 22, 2024 that certain files in the email account containing your personal information may have been accessed and/or acquired by the unauthorized party.

What Information Was Involved?

The impacted data contained some of your personal information, including your full name and address, date of birth, medical treatment information, health insurance information, provider, and/or diagnosis information.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

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

For More Information.

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 1-800-405-6108. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday 8 am to 8 pm Eastern Standard Time, excluding major U.S. holidays.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

Sincerely,

City of Conneaut

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

We recommend that you place a one-year “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
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329

Experian

P.O. Box 9554
Allen, TX 75013
www.experian.com/fraud/center.html
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-alerts
(800) 680-7289

2. 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
www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/center.html
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(888) 916-8800

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. 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 a credit monitoring service, 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.

3. 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.

4. Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

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.

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, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.