

Nicholas A. Kurk
Direct Dial: 312-642-6738
E-mail: nkurk@mcdonaldhopkins.com

October 17, 2024

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

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

Re: The City of Coon Rapids, MN - Incident Notification

Dear Mr. Brown:

McDonald Hopkins LLC represents the City of Coon Rapids, MN (“the City”), located at 11155 Robinson Drive NW, Coon Rapids, MN 55433. I am writing to provide notification of an incident at the City that may affect the security of personal information of two (2) Maryland residents. By providing this notice, the City does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about June 2, 2024, an unauthorized party acquired a limited number of files from the City of Coon Rapids’ computer systems. Upon detecting the unauthorized activity, the City of Coon Rapids immediately contained the incident and commenced an immediate and thorough investigation. As part of its investigation, the City engaged leading cybersecurity experts to identify what personal information, if any, was involved. After an extensive forensic investigation and document review, the City concluded, on or about September 18, 2024, that one or more of the files that may have been accessed and/or acquired by an unauthorized individual(s) contained personal information about Maryland residents. The personal information contained within the impacted data included first and last name, Social Security number, and financial account information. The types of impacted information varied by individual.

The City has no evidence of financial fraud or identity theft related to this data. Nevertheless, out of an abundance of caution, the City wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. The City is providing the affected residents with notification of this incident, commencing on or about October 17, 2024. The notice will be in substantially the same form as the letter attached hereto. The City is also offering the affected residents a complimentary membership with a credit monitoring service. The City is advising the affected residents to always remain vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. The

October 17, 2024

Page 2

City is also advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected residents are being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

If you have any additional questions, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com.

Very truly yours,



Nicholas A. Kurk

Encl.



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



Enrollment Code:

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:

October 17, 2024



Dear

We are writing to inform you of a data security incident at the City of Coon Rapids, MN (the “City”) involving some of your information. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about June 2, 2024, an unauthorized party acquired a limited number of files from our computer systems.

What We Are Doing.

Upon detecting the unauthorized activity, we immediately contained the incident and commenced an immediate and thorough investigation. As part of our investigation, the City engaged leading cybersecurity experts to identify what personal information, if any, was involved.

What Information Was Involved?

After an extensive forensic investigation and document review, the City concluded on or about September 18, 2024 that one or more of the files potentially acquired by the unauthorized party contained

What You Can Do.

The City has no evidence of any identity theft or financial fraud directly related to this incident. Out of an abundance of caution to protect you from potential misuse of your information, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity-theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on identity theft prevention

and credit monitoring, including instructions on how to activate your complimentary 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 Security Freeze on your credit files, and 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.

Please accept our apologies that this incident occurred. The City is 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.

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]. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of [REDACTED].

Sincerely,

A handwritten signature in dark ink, appearing to read "Matt Stumm". The signature is written in a cursive, flowing style.

City Manager

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary <<12/24>> months Credit Monitoring

- **Deadline:** Please note the deadline to enroll is [REDACTED].
- **Website and Enrollment.** Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Contact IDX with any questions and to enroll in free identity protection services by calling [REDACTED], going to [REDACTED] or scanning the QR image and using the Enrollment Code provided above.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary <<12/24>> month credit monitoring services, we recommend that you place an initial 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 (1) of the three (3) 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.

Additionally, you may request delivery of an investigation report related to this incident by physical mail or email. To request a copy of the investigation report, please send a written request via mail to the City of Coon Rapids Clerk's Office at 11155 Robinson Drive, Coon Rapids, MN 55433 or via email to investigativereport@coonrapidsmn.gov

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

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.

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: 1-877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392