

# McDonald Hopkins

A business advisory and advocacy law firm®

**Heather Shumaker**

Direct Dial: 248.402.4066

E-mail: [hshumaker@mcdonaldhopkins.com](mailto:hshumaker@mcdonaldhopkins.com)

McDonald Hopkins PLC  
39533 Woodward Avenue  
Suite 318  
Bloomfield Hills, MI 48304

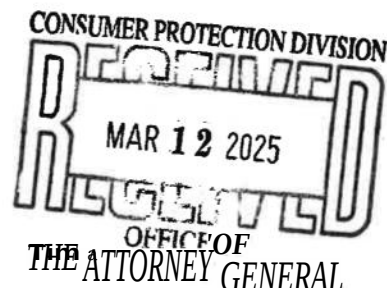
P 1.248.646.5070

F 1.248.646.5075

March 7, 2025

**VIA EMAIL ([IdtheKa.oag.state.md.us](mailto:IdtheKa.oag.state.md.us))**

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



**Re: Jewish Community Center of Greater Rochester – Incident Notification**

Dear Mr. Brown:

McDonald Hopkins PLC represents the Jewish Community Center of Greater Rochester (“JCC of Greater Rochester”). I am writing to provide notification of an incident the JCC of Greater Rochester experienced that may affect the security of personal information of approximately three (3) Maryland residents. By providing this notice, JCC of Greater Rochester does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

JCC of Greater Rochester recently received notice from one of its accounting vendors, indicating that it had inadvertently sent a document containing personal information belonging to a limited number of JCC of Greater Rochester’s contracted employees to other clients and the accounting vendor confirmed each recipient deleted the file. There was no compromise to JCC of Greater Rochester’s network environment.

Upon learning of this issue, JCC of Greater Rochester commenced a prompt and thorough investigation. As part of the investigation, JCC of Greater Rochester has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive investigation and document review, on February 7, 2025, JCC of Greater Rochester identified the contracted employees whose personal information was inadvertently shared by MMB. The information included the impacted residents Social Security number.

To date, JCC of Greater Rochester is not aware of any reports of identity fraud or improper use of information as a direct result of this incident. Nevertheless, JCC of Greater Rochester 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. JCC of Greater Rochester is

providing the affected residents with written notification of this incident commencing on or about March 7, 2025 in substantially the same form as the letter attached hereto. JCC of Greater Rochester is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are being offered complimentary credit monitoring for one year. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission and the Maryland Attorney General.

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

Should you have any questions regarding this notification, please contact me at 248.402.4066 or [hshumaker@mcdonaldhopkins.com](mailto:hshumaker@mcdonaldhopkins.com). Thank you for your cooperation.

Very truly yours,

A handwritten signature in black ink, appearing to read 'H. Shumaker', with a long horizontal flourish extending to the right.

Heather Shumaker

HS/cs



[REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to the Jewish Community Center of Greater Rochester, Inc ("JCC of Greater Rochester"). We write to make you aware of a recent data security incident involving a third-party vendor that impacted some of your personal information. We want to provide you with details about the incident, share information about 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 January 15, 2025, JCC of Greater Rochester received notice from one of its accounting vendors who relayed that they had inadvertently sent a document containing personal information belonging to a limited number of JCC of Greater Rochester's contracted employees to other clients. The accounting vendor confirmed that each recipient deleted the file. There was no compromise to JCC of Greater Rochester's network environment.

**What We Are Doing.**

Upon being informed of the incident, JCC of Greater Rochester immediately took actions to assess the scope of information potentially compromised, including engaging third-party professionals to assist in an investigation of the incident. Following the investigation and notification from our vendor, we determined on February 7, 2025, that your personal information was included in the file that was mistakenly shared. To date, JCC of Greater Rochester is not aware of any reports of identity fraud or financial fraud for any information as a direct result of this incident.

**What Information Was Involved?**

The potentially impacted information includes your full name and [REDACTED].

**What You Can Do.**

JCC of Greater Rochester has no information that any of your information has been misused. We are offering a complimentary [REDACTED]-month membership to [REDACTED] services at no charge. These services provide you with alerts for [REDACTED] 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. These services will be provided by [REDACTED] company specializing in fraud assistance and remediation services.

For more information on the services available and how to enroll, please see the Other Important Information page which 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 on a regular basis.

**For More Information.**

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, including a review of our ongoing third-party vendor relationships.

If you have any further questions regarding this incident please contact [REDACTED] at [REDACTED].

JCC of Greater Rochester  
1200 Edgewood Avenue  
Rochester, NY 14618

**– OTHER IMPORTANT INFORMATION –**

**1. Enrolling in Complimentary [REDACTED]-Month 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. Obtain and Monitor Your Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies. You can obtain a free copy of your credit report by calling **1-877-322-8228**, visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), 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 access the request form at <https://www.annualcreditreport.com/index.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below.

***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

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.

**3. Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name.

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. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>.

***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

**4. Placing a Security Freeze on Your Credit File.**

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

***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 will 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 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.

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.

**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](http://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.

**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](http://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.

**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/](http://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.