



A business advisory and advocacy law firm®

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

McDonald Hopkins LLC
300 N. LaSalle Street
Suite 1400
Chicago, IL 60654

P 1.312.280.0111
F 1.312.280.8232

August 14, 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: Beth Rogers Agency – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents the Beth Rogers Agency (the “Agency”). I am writing to provide notification of an incident at the Agency that may affect the security of personal information of approximately 12 Maryland residents. The Agency investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, the Agency does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On May 10, 2024, the Agency became aware of potentially unauthorized access to a single Agency email account. The Agency immediately commenced a prompt and thorough investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations. The investigation did not identify evidence of specific data access or acquisition by an unauthorized party, but could not conclude with one-hundred percent certainty that data within the email account was not accessed or acquired by an unauthorized party. Therefore, out of an abundance of caution, the Agency conducted an extensive review of the email account to determine what data may have been present within the email account. After this extensive forensic investigation and manual document review of all emails and any attachments, the Agency discovered on July 29, 2024 that certain emails or attachments within the email account contained a limited amount of personal information. Notification to certain persons and regulators is, therefore, being provided out of an abundance of caution. The personal information which may have been accessed by the unauthorized party included the affected residents’ full names and Social Security numbers.

To date, the Agency 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, the

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

mcdonaldhopkins.com

33383979.1
34053469.1

Page 2

Agency 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 Agency is providing the affected residents with written notification of this incident commencing on or about August 14, 2024 in substantially the same form as the letter attached hereto. The Agency is offering the affected residents whose Social Security numbers were impacted complimentary memberships with a credit monitoring service. The Agency 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 also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

Should you have any questions concerning this notification, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in black ink, appearing to read 'N. A. Kurk', with a stylized, cursive script.

Nicholas A. Kurk

Encl.

Beth Rogers Agency Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: [REDACTED]

Visit
[REDACTED]

[REDACTED]

August 14, 2024

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to the Beth Rogers Agency Inc. We are writing with important information regarding a recent data security incident. We want 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 May 10, 2024, we became aware of potentially unauthorized access to an email account of one Beth Rogers Agency Inc. employee.

What We Are Doing.

Upon detecting the incident, we immediately commenced a prompt and thorough investigation, which included containing and securing the email environment, and changing account passwords. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents to investigate the extent of the incident and what, if any, sensitive data, including personal and/or health information may have been accessed and/or acquired by the unauthorized party. The investigation did not identify evidence of specific data access or acquisition by an unauthorized party, but could not conclude with one-hundred percent certainty that data within the email account was not accessed or acquired by an unauthorized party. Therefore, out of an abundance of caution, we conducted an extensive review of the email account to determine what data may have been present within the email account. After this extensive forensic investigation and manual document review of all emails and any attachments, we discovered on July 29, 2024 that certain emails or attachments within the email account contained personal information.

What Information Was Involved?

The information potentially involved includes your full name and [REDACTED]

What You Can Do.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Nevertheless, to protect you from potential misuse of your information, we are providing you with identity theft protection services through [REDACTED], the data breach and recovery services expert. [REDACTED]

identity protection services include: [REDACTED] of credit and [REDACTED] monitoring, a \$ [REDACTED] [REDACTED], and [REDACTED]. With this protection, IDX will help you resolve issues if your identity is compromised.

This letter also provides other precautionary measures to protect your personal information, including placing a fraud alert, placing a security freeze, 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.

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.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [REDACTED], or by going to [REDACTED] and using the Enrollment Code provided here: [REDACTED]. IDX representatives are available Monday through Friday from [REDACTED] Eastern Time. Please note the deadline to enroll is [REDACTED].

Sincerely,

The Beth Rogers Agency Inc.

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [REDACTED]-Month Credit Monitoring.

Website and Enrollment. Go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided on page 2 of the letter.

Activate the credit monitoring provided as part of your [REDACTED] 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, [REDACTED] will be able to assist you.

Telephone. Contact [REDACTED] at [REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. 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 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
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 685-1111

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 charge. 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 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’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 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.

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.

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.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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.

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.

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.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

*In Addition, New Mexico Consumers Have the Right to
Obtain a Security Freeze or Submit a Declaration of Removal*

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.