

R. David Lane, Esq.
Direct Dial: 248.402.4072
E-mail: dlane@mcdonaldhopkins.com

September 27, 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: Scott Richards Agency – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents the Scott Richards Agency (the “Agency”). I am writing to provide notification of an incident at the Agency that may affect the security of personal information of one (1) Maryland resident. 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 April 16, 2024, the Agency became aware of potentially unauthorized access to a single Agency email account. The Agency immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information contained in the impacted account. Based on its comprehensive investigation and document review, the Agency discovered on August 28, 2024 that certain files in the impacted account containing personal information may have been accessed and acquired by the unauthorized party in connection with this incident, including the affected resident’s full name and Driver’s License or State Issued ID Number.

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 Agency 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. The Agency is providing the affected resident with written notification of this incident commencing on or about September 27, 2024 in substantially the same form as the letter attached hereto. The Agency is advising the affected resident about the process for placing fraud alerts and/or security freezes on

Page 2

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 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 (248) 402-4072 or dlane@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in black ink, appearing to read "R. David Lane, Esq.", written in a cursive style.

R. David Lane, Esq.

Encl.



SAVEONINSURANCE

[REDACTED]

[REDACTED]

September 27, 2024

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to the Scott Richards Agency. We are writing with important information regarding a recent data security incident. We want 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 April 16, 2024, we became aware of potentially unauthorized access to the email account of a single Scott Richards Agency 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 information may have been accessed and/or acquired by the unauthorized party. After an extensive forensic investigation and manual document review, we discovered on August 28, 2024 that certain emails or attachments within the email account contained personal information. On September 19, 2024 we confirmed your address and promptly took steps to notify you.

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, out of an abundance of caution, this letter provides 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 by calling our dedicated call center at [REDACTED]. IDX representatives are available Monday through Friday from [REDACTED] - [REDACTED] Pacific Time.

Sincerely,

The Scott Richards Agency



Scott Richards

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

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

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 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.

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. 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, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

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.