

Eric R. Benson
Direct Dial: 248.593.2957
E-mail: ebenson@mcdonaldhopkins.com

March 17, 2025

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

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

Re: Mark Thomas – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Mark Thomas (located at 2833 Junction Avenue, Suite 110, San Jose, CA 95134). I am writing to provide notification of a cybersecurity incident that impacted Mark Thomas and may affect the security of personal information of on or about one (1) Maryland resident. By providing this notice, Mark Thomas does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about October 19, 2024, Mark Thomas identified unusual activity on its network. Upon identifying the activity, Mark Thomas acted quickly to contain the threat and conduct a privileged investigation with the assistance of third-party forensic specialists. The investigation revealed that between on or about October 11, 2024 to on or about October 19, 2024, an unauthorized individual accessed its systems. Mark Thomas' review concluded recently and discovered on or about February 19, 2025 that personal information was included within the data that may have been viewed or acquired by the unauthorized actor. Further, on or about March 10, 2025, Mark Thomas located the most recent contact information for these individuals and identified approximately one (1) Maryland resident whose information was involved. The personal information contained within the impacted data included first and last name and Social Security number.

Mark Thomas has no evidence of financial fraud or identity theft related to this data. Nevertheless, out of an abundance of caution, Mark Thomas 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. Mark Thomas is providing the affected resident with notification of this incident, commencing on or about March 17, 2025. The notice will be in substantially the same form as the letter attached hereto. Mark Thomas is also offering the affected resident whose Social Security number was potentially impacted by the incident with complimentary one-year membership with a credit monitoring service. Mark Thomas is advising the affected resident to always remain vigilant in reviewing financial account statements,

March 17, 2025

Page 2

explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. Mark Thomas is also advising the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected resident is being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (248) 593-2957 or email me at ebenson@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink, consisting of stylized initials 'EB' followed by a horizontal line.

Eric R. Benson

Encl.

Mark Thomas
c/o Cyberscout



[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

March 17, 2025

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to Mark Thomas. We are writing with important information regarding a recent data security incident that may have involved some of your personal information. 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 personal information.

What Happened?

On or around October 19, 2024, Mark Thomas became aware of potential unauthorized access on our network.

What We Are Doing

Upon learning of this issue, we took steps to ensure the security of our systems, and we commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals experienced in handling these types of situations to assist us in determining the full extent of the incident and the scope of any data impacted. Our investigation revealed that an unauthorized actor accessed our systems from on or about October 11, 2024, to on or about October 19, 2024, and, as a result, possibly viewed and/or obtained certain files containing some of your personal information.

On or about February 19, 2025, after an extensive forensic investigation and manual document review, we discovered your personal information was included within the impacted data that may have been copied from our network as a result of the incident.

What Information Was Involved

The impacted files contained your [REDACTED]
[REDACTED].

What You Can Do

While we have no evidence of financial fraud or identity theft related to the impacted information, out of an abundance of caution to protect you from potential misuse of your information, we are offering a complimentary 12 months membership for credit monitoring. 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, explanation of benefits 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.

If you have any further questions regarding this incident, please call the dedicated, confidential toll-free response line we have set up to respond to questions at [REDACTED]. The response line is staffed with professionals familiar with this incident and knowledgeable about what you can do to protect against misuse of your information. The response line is available between the hours of [REDACTED], Monday through Friday, excluding holidays.

Sincerely,

Mark Thomas

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 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 Cyberscout, a TransUnion company.

How do I enroll for the free services?

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 [REDACTED] 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. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) 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) 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. 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 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. Protecting Your Health Information.

The following practices can help to protect you from 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.

6. 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.



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.

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.

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.

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.

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: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

