

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

March 12, 2025

VIA ELECTRONIC MAIL: (Idtheft@oag.state.md.us)

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

Re: Luminis Health, Inc. – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Luminis Health, Inc. (“Luminis Health”). Headquartered in Annapolis, Maryland,¹ Luminis Health is a non-profit provider of healthcare services. I am writing to provide notification of an incident at Luminis Health that may affect the security of personal information of approximately three-hundred forty-nine (349) Maryland residents. By providing this notice, Luminis Health does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Luminis Health recently determined that, on or about December 16, 2024, an unauthorized party obtained access to a third-party consultant’s account and accessed our payroll software system on or about December 11, 2024. Upon detecting the unauthorized activity, Luminis Health immediately contained the incident and commenced a thorough investigation. As part of its investigation, Luminis Health engaged leading cybersecurity experts to identify what personal information, if any, was involved.

On or about January 25, 2025, Luminis Health discovered that the unauthorized party accessed and potentially acquired personal information pertaining to a limited number of individuals from the payroll software system such as full names, bank account number, and bank routing number. The elements of information varied per individual, and, for a limited number of individuals, Social Security numbers were also potentially involved. Although the investigation did not identify whether the unauthorized party acquired the personal information, out of an abundance of caution and for purposes of full transparency, we are notice of the underlying incident.

Luminis Health has no evidence of any identity theft or financial fraud related to this incident. Nevertheless, out of an abundance of caution, Luminis Health wanted to inform you of

¹ 2001 Medical Parkway, Annapolis, Maryland 21401

March 12, 2025

Page 2

the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud.

Luminis Health is providing the affected residents with written notification of this incident commencing on or about March 11, 2025 in substantially the same form as the letter attached hereto. Luminis Health will advise the affected individuals to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The affected individuals will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. The impacted individuals will be provided a complimentary one-year membership with a credit monitoring service.

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

If you have any additional questions, please contact me at (410) 456-2741 or spollock@mcdonaldhopkins.com.

Very truly yours,



Spencer S. Pollock

SPP/efg

Exhibit A



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



March 11, 2025

***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

Dear [REDACTED]:

We are writing with important information regarding a recent security incident at Luminis Health, Inc. 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?

We recently learned that an unauthorized party obtained access to an outside third-party consultant's account and accessed our payroll software system on or about December 11, 2024. Please note the payroll software system had yet to be rolled out at the time of the underlying incident.

What We Are Doing.

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we are working very closely with external cybersecurity professionals. On or about December 16, 2024, we discovered that the unauthorized party accessed and potentially acquired some of your personal information from the payroll software system. Although the investigation did not identify whether the unauthorized party acquired your personal information, out of an abundance of caution and for purposes of full transparency, we are offering the credit monitoring services described in detail below.

What Information Was Involved?

The impacted payroll software system contained some of your personal information, including your [REDACTED]
[REDACTED].

What You Can Do.

Out of an abundance of caution, we are also offering 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 [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. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, 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.

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]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday, 9 am – 9 pm Eastern Time.

Sincerely,

Ron Nolte
Chief Information Officer
Luminis Health, Inc.

Amy Beales
Chief Human Resources Officer
Luminis Health, Inc.

– 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. If you would like to enroll over the phone, please call [REDACTED]. 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 by April 17, 2025. 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.

Whether or not you choose to use the complimentary [REDACTED]-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 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. 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.

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.