

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

January 30, 2025

VIA EMAIL (Idtheft@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: Lucent Health Solutions – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Lucent Health Solution, Inc. (“Lucent Health”). I am writing to provide notification of an incident at Lucent Health that may affect the security of personal information of twenty one (21) Maryland residents. By providing this notice, Lucent Health does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On October 2, 2023, a Lucent Health manager opened a single “phishing” email from a trusted broker. Lucent Health’s IT Team identified suspicious activity on the employee’s email account, and eliminated access within approximately ninety (90) minutes. Lucent Health commenced an immediate and thorough investigation. After an extensive investigation, Lucent Health determined that one e-mail account was subject to unauthorized access for a limited period (approximately ninety (90) minutes), and that the unauthorized individual queried select search terms. **The cybersecurity firm did not identify evidence that the unauthorized individual obtained information from the e-mail account or that they actually viewed any information.** Lucent Health, however, cannot confirm if certain e-mails and information were accessed.

As such, out of an abundance of caution, on June 28, 2024, Lucent Health posted a website notice regarding the incident. After a thorough review of the impacted documents, Lucent Health notified the covered entities of the incident on December 3, 2024 and provided these entities with a list of potentially impacted individuals. On January 22, 2025, Lucent Health determined the most recent contact information of the potentially impacted individuals. On January 30, 2025, Lucent Health notified certain individuals about a data security incident that potentially impacted their personal and health information.

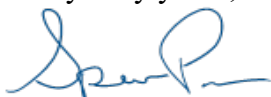
Lucent Health has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, Lucent Health is providing notice

to the affected residents commencing on January 30, 2025 in substantially the same form as the document attached hereto. Lucent Health is also offering complimentary credit monitoring to the impacted residents who had their Social Security number impacted. Additionally Lucent Health will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Lucent Health will further advise the affected residents about the process for placing a fraud alert and/or security freeze 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 Lucent Health, protecting the privacy of personal information is a top priority. Lucent Health is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Lucent 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,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock".

Spencer S. Pollock

Encl.

Lucent Health Solutions, LLC



January 30, 2025

RE: [REDACTED]

Dear [REDACTED]:

We are writing with important information regarding a recent cyber security incident at Lucent Health Solutions, LLC ("Lucent Health") that may involve your personal information. We wanted to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On October 2, 2023, a Lucent Health manager opened a single "phishing" email from a trusted broker. Lucent Health's IT Team identified suspicious activity on the employee's email account, and eliminated access within approximately ninety (90) minutes.

What We Are Doing

Upon learning of this issue, we immediately commenced a prompt and thorough investigation working very closely with external cybersecurity professionals experienced in handling these types of incidents to determine whether there was any unauthorized access to protected information.

After an extensive forensic investigation, Lucent Health determined that one e-mail account was subject to unauthorized access for a limited period (approximately ninety (90) minutes), and that the unauthorized individual queried select search terms. **The cybersecurity firm confirmed no information was downloaded or electronically transferred from the email account, and they did not identify evidence that the unauthorized individual actually viewed any information.** Out of an abundance of caution, we wanted to notify you about the incident.

What Information Was Involved?

The potentially accessed information includes your full name and date of birth, Social Security number, and health, dental, and vision group and/or plan number.

What You Can Do

Once again, we have no evidence that the information was obtained or actually viewed or that any information has been misused.

Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, 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 24 months from the date of enrollment when changes occur to your credit file.

000010102G0400

P

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 specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> 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.

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

We sincerely regret that this incident occurred. We have taken many precautions to safeguard your information and continually evaluate and modify our practices and internal controls accordingly. **If you have additional questions regarding this notice, please direct them to 1-833-961-7569 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.**

Sincerely,

Lucent Health Solutions, Inc.
424 Church St #2300
Nashville, TN 37219

- OTHER IMPORTANT INFORMATION -

1. 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**, 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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the 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

3. 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.

Protecting Your Medical Information.

As a general matter, 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.

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, 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. **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.