

**Dominic A. Paluzzi**  
Direct Dial: 248-220-1356  
Email: [dpaluzzi@mcdonaldhopkins.com](mailto:dpaluzzi@mcdonaldhopkins.com)

September 11, 2024

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

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

**Re: Plastic Surgery Chicago, LLC – Incident Notification**

To Whom It May Concern:

McDonald Hopkins PLC represents Plastic Surgery Chicago, LLC (“Plastic Surgery Chicago”). Located in Chicago, Illinois,<sup>1</sup> I am writing to provide notification of an incident at Plastic Surgery Chicago that may affect the security of personal information of approximately one (1) Maryland resident. By providing this notice, Plastic Surgery Chicago does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

We recently determined that an electronic storage device maintained by Plastic Surgery Chicago, LLC was potentially acquired by an unauthorized party on or about July 3, 2024. Upon learning of the issue, Plastic Surgery Chicago commenced a prompt and thorough investigation.

After an investigation and internal review, Plastic Surgery Chicago discovered on or about August 16, 2024 that the storage device that was potentially accessed contained protected health information pertaining to a limited number of individuals, such as full names, dates of birth, medical treatment information, and/or images. The elements of information potentially involved varied per individual. Plastic Surgery Chicago have no evidence that any of the information has been misused.

Plastic Surgery Chicago has no evidence of any identity theft or financial fraud related to this incident. Nevertheless, out of an abundance of caution, Plastic Surgery Chicago wanted to inform you of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud.

Plastic Surgery Chicago is providing the affected residents with written notification of this incident commencing on or about September 11, 2024 in substantially the same form as the letter attached hereto. Plastic Surgery Chicago will advise the affected individuals to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a

---

<sup>1</sup> 60 East Delaware Place, Suite 1430, Chicago, IL 60611

September 11, 2024

Page 2

regular basis. The affected individuals will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Plastic Surgery Chicago, protecting the privacy of personal information is a top priority. Plastic Surgery Chicago is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Plastic Surgery Chicago 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 (248) 220-1356 or [dpaluzzi@mcdonaldhopkins.com](mailto:dpaluzzi@mcdonaldhopkins.com).

Very truly yours,



Dominic A. Paluzzi

DP/erb

## **Exhibit A**

Robert L. Walton, MD, FACS



**IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY**

Dear [REDACTED]:

We are writing to inform you of a data security incident at Plastic Surgery Chicago, LLC involving some of your information. We wanted 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?*

We recently determined that an electronic storage device maintained by Plastic Surgery Chicago, LLC was potentially acquired by an unauthorized party on or about July 3, 2024.

*What We Are Doing.*

Upon learning of the issue, we commenced a prompt and thorough investigation. After an investigation and internal review, we discovered on or about August 16, 2024 that the storage device that was potentially acquired contained some of your protected health information.

*What Information Was Involved?*

The storage device that may have been acquired contained some of your protected health information, potentially including your [REDACTED].

*What You Can Do.*

We have no evidence that any personal information has been or will be misused as a direct result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and provide you with steps you can take to protect your information further. This letter 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 and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages.

*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.

[REDACTED]

**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 protect against misuse of your information. The response line is available Monday through Friday, 8:00 am to 8:00 pm Eastern Time.

Sincerely,

Robert L. Walton, MD  
Plastic Surgery Chicago, LLC

- OTHER IMPORTANT INFORMATION -

**1. Placing a Fraud Alert.**

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-alert>  
s  
(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 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>  
eze  
(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.

**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.



00001020280000

P

#### 4. **Protecting Your Medical Information.**

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter the following practices can provide additional safeguards to protect you against 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](http://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.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://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.

**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/](http://www.ncdoj.gov/), Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.