

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

November 20, 2023

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

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

Re: Proliance Surgeons – Incident Notification

Dear Attorney General Moody:

McDonald Hopkins PLC represents Proliance Surgeons (“Proliance”). I am writing to provide notification of an incident at Proliance that may affect the security of personal information of one (1) Maryland resident. By providing this notice, Proliance does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Proliance detected that certain systems within its network had been affected by a ransomware attack. The incident resulted in the unauthorized access and/or acquisition of certain files from the network, which occurred on February 11, 2023. Upon detecting the incident, Proliance commenced an immediate and thorough investigation, contained the network, and alerted law enforcement. On February 27, 2023, Proliance determined certain personal information for a limited number of patients was affected by the incident. Proliance notified these patients on March 22, 2023.

As part of the investigation, Proliance engaged third party cybersecurity professionals to investigate the extent of the activity and what, if any, additional individual personal information may have been accessed and/or acquired by an unauthorized party. On May 24, 2023, Proliance discovered that certain additional files involved in the incident could have contained personal information, but had not yet identified the specific individuals involved. As a result, Proliance posted a notice to its website about the incident on July 18, 2023, and included steps individuals could take to protect their personal information. Proliance conducted a detailed and comprehensive review of all the data involved, and determined on September 22, 2023 the specific individual personal information present in the files potentially accessed and/or acquired by an unauthorized party. Proliance promptly moved to notify individuals via letter.

Proliance has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, Proliance 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. Proliance is providing the affected resident with written notification of this incident commencing on or about November 20, 2023 in substantially the same form as the letter attached hereto. Proliance will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Proliance will also advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Proliance, protecting the privacy of personal information is a top priority. Proliance is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Proliance 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) 917-5189 or spollock@mcdonaldhopkins.com.

Very truly yours,



Spencer S. Pollock

Encl.

Proliance Surgeons
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***



November 20, 2023

Dear [REDACTED]

Proliance Surgeons ("Proliance") is committed to our patients, their treatment, and their families – as well as protecting the privacy and security of their personal information. We are writing with important information regarding a data security incident that may have affected your personal information. The privacy and security of the information we maintain is of the utmost importance to Proliance Surgeons. 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?

Proliance detected that certain systems within our network had been affected by a cybersecurity incident. The incident resulted in the potential unauthorized access and/or acquisition of certain files from the network, which occurred on February 11, 2023.

What We Are Doing

Upon detecting the incident, Proliance commenced an immediate and thorough investigation, contained the network, alerted law enforcement, and notified certain individuals whose personal information was present in the above-mentioned files. As part of our investigation, Proliance engaged third party cybersecurity professionals to investigate the extent of the activity and what, if any, additional individual personal information may have been accessed and/or acquired by an unauthorized party. On May 24, 2023, we discovered that certain additional files involved in the incident could have contained personal information but had not yet identified the specific individuals involved. As a result, we posted a notice to our website about the incident, and included steps individuals could take to protect their personal information. We conducted a detailed and comprehensive review of all the data involved, and determined on September 22, 2023 that your information was present in the additional files potentially accessed and/or acquired by an unauthorized party. We immediately took steps to notify you of the incident and provide you with information to safeguard your personal information.

What Information Was Involved?

The information potentially involved includes your name and Date of Birth.

What You Can Do

This letter also provides other precautionary measures you can take to protect your 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, explanation of benefits, and credit reports for fraudulent or irregular activity on a regular basis.

000010102G0500

P

For More Information

Proliance values your privacy and deeply regrets that this incident has occurred. We take the security of your information very seriously and have taken many additional precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your information. Since detecting the incident, we have reviewed and revised our information security practices, and implemented additional security measures to mitigate the chance of a similar event in the future.

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

Sincerely,

Proliance Surgeons

OTHER IMPORTANT INFORMATION

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial 90-day “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



2. 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.

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. Protecting Your Health 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 the 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 disclosure (February 11, 2023) 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 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.

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.

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.

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.

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.