



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory Lederman
Office: (267) 930-4637
Fax: (267) 930-4771
Email: glederman@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 18, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Orthopaedic Associates of Allentown d/b/a OAA Orthopaedic Specialists (“OAA”), located at 250 Cetronia Rd, Suite A, Allentown, PA 18104, and are writing to notify your Office of an incident that may affect the security of information relating to twenty (20) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, OAA does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 24, 2021, OAA became aware of suspicious activity related to certain internal computer systems and servers. OAA immediately took steps to secure its network, minimize any disruption to operations, and launched an investigation with the assistance of third-party forensic and cybersecurity specialists into the nature and scope of the event. Through this investigation, OAA determined that an unauthorized actor placed malware within the OAA environment that disrupted operations of certain OAA systems. The investigation further determined that the unauthorized actor may have accessed or acquired certain information contained in impacted OAA systems between September 17, 2021 and September 24, 2021. On or about October 25, 2021, the investigation determined that certain OAA employee and patient information may be impacted as a result of this event. Thereafter, OAA conducted a thorough internal review, which concluded on December 9, 2021, in order to determine those individuals whose information was present on the impacted systems at the time of the event and to identify address information in order to provide

them with notice of the event. While the information varies for each individual, the information that could have been subject to unauthorized access includes name, date of birth, health insurance information, and medical record number.

Notice to Maryland Residents

On or about November 23, 2021, OAA began notifying potentially affected individuals while the investigation was ongoing. On or about January 18, 2022, OAA provided written notice of this incident to affected individuals, which includes twenty (20) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, OAA moved quickly to investigate and respond to the incident, assess the security of OAA systems, and notify potentially affected individuals. OAA is also working to implement additional safeguards and training to its employees.

Additionally, OAA is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and Explanation of Benefits, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4637.

Very truly yours,

Gregory Lederman of
MULLEN COUGHLIN LLC

GCL/ams
Enclosure

EXHIBIT A



Orthopaedic Specialists

Return Mail Processing Center

P.O. Box 6336

Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

<<Variable Text 2>>

Dear <<Name 1>>:

Orthopaedic Associates of Allentown dba OAA Orthopaedic Specialists (“OAA”) is writing to inform you of a recent incident that may affect the security of some of your information. While we are not aware of any actual or attempted misuse of your information, we are providing you with an overview of the incident, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it necessary to do so.

What Happened? On September 24, 2021, OAA became aware of suspicious activity related to certain internal computer systems and servers. We immediately took steps to secure our network, minimize any disruption to operations, and launched an investigation with the assistance of third-party forensic and cybersecurity specialists in the nature and scope of the event. Through this investigation, we determined that an unauthorized actor placed malware within the OAA environment that disrupted operations of certain OAA systems. The investigation further determined that the unauthorized actor may have accessed or acquired certain information contained in impacted OAA systems between September 17, 2021 and September 24, 2021. On or about October 25, 2021, the investigation determined that certain OAA patient information may be impacted as a result of this event.

What Information Was Involved? Upon learning this information, we began an in-depth manual review of the impacted files in order to confirm the presence of patient information. While this review is ongoing, OAA is notifying you out of an abundance of caution because the investigation determined that your <<Variable Text 1>> was present in the impacted files at the time of the incident. To date, OAA has not received any reports of actual or attempted misuse of your information.

What We Are Doing. We take this incident and the security of patient information within our care very seriously. In addition to the steps described above, as part of our ongoing commitment to the privacy of information in our care, we are working to review our existing policies and procedures, to provide additional training programs to employees, and are implementing additional safeguards to further secure the information in our systems.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, monitoring your free credit reports and Explanation of Benefits for suspicious activity, and to detect errors over the next 12 to 24 months. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 855-604-1699, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

OAA Orthopaedic Associates

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. OAA is located at 250 Cetronia Rd, Suite A, Allentown, PA 18104.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting

agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is/are approximately 1 Rhode Island residents impacted by this incident.