

May 31, 2022

Tawana B. Johnson, Esq.
470.419.6653 (direct)
Tawana.Johnson@WilsonElser.com

Via electronic-mail: Idtheft@oag.state.md.us

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

Re:	Our Client	:	Associated Ophthalmologists of Kansas City, P.C.
	Matter	:	Data Security Incident on December 4, 2021
	Wilson Elser File #	:	16516.01801

Dear Attorney General Frosh:

We represent Associated Ophthalmologists of Kansas City, P.C. (“AOKC”) headquartered in Kansas City, Missouri, with respect to a potential data security incident described in more detail below. AOKC takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of Maryland residents that were potentially affected, what information has been compromised, and the steps that AOKC is taking to secure the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

In 2021, Associated Ophthalmologists of Kansas City, P.C. (“AOKC”) was using the electronic medical records platform “myCare Integrity,” which was provided by the practice performance company Eye Care Leaders (“ECL”). AOKC trusted Eye Care Leaders to protect its patient’s data, and had electronic medical records for many of its patients stored on the Eye Care Leaders platform.

According to Eye Care Leaders, on or around December 4, 2021, an unauthorized party accessed myCare Integrity data and deleted databases and system configuration files. There was no evidence that this incident involved unauthorized access to any of AOKC’s patient records. On April 19, 2022, Eye Care Leaders notified AOKC that a lack of available forensic evidence prevented Eye Care Leaders from ruling out the possibility that some protected health information and personally

3348 Peachtree Road N.E., Suite 1400 • Atlanta, Georgia 30326 • p 470.419.6650 • f 470.419.6651

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Seattle • Stamford • Virginia • Washington, DC • Wellington • White Plains •

wilsonelser.com

identifiable information may have been exposed to the bad actor. The lack of forensic evidence provided by Eye Care Leaders has put AOKC in a position where it is impossible to determine whether or not a breach of its patient information occurred at all. Although there was no evidence that any patient data was compromised, and we believe there is a low probability of PHI exposure, AOKC has decided to notify its patients out of an abundance of caution.

2. Maryland Residents Notified

A total of one (1) resident of Maryland was potentially affected by this security incident. A notification letter to this individual will be mailed on May 31, 2022, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

This data security incident occurred entirely within Eye Care Leaders' network environment, and there were no other remedial actions available to AOKC.

Although AOKC is not aware of any evidence of misuse of personal information, AOKC extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service will include 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise. The notification letter and offer of free credit monitoring will be mailed on May 31, 2022.

4. Contact Information

AOKC remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Tawana.Johnson@WilsonElser.com or 470.419.6653.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Tawana B. Johnson, Esq.

Copy: Robert Walker, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*

AOKC
Associated Ophthalmologists
of Kansas City, P.C.
P.O Box 989728
West Sacramento, CA 95798-9728

To enroll, please call: 1-833-909-4428

Or Visit: <https://app.idx.us/account-creation/protect>

Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

May 31, 2022

Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

Associated Ophthalmologists of Kansas City, P.C. ("AOKC") is an ophthalmology clinic located in Kansas City, Missouri. In 2021, AOKC was using the electronic medical records platform "myCare Integrity," which was provided by the practice performance company Eye Care Leaders ("ECL"). We are writing in order to inform you that some of your sensitive personal information may have been stored on the myCare Integrity system at the time of a data security incident suffered by Eye Care Leaders in 2021. This is a precautionary notice, and we have no evidence to suggest that your personal information was actually compromised. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

According to Eye Care Leaders, on or around December 4, 2021, an unauthorized party accessed myCare Integrity data and deleted databases and system configuration files. According to Eye Care Leaders, upon identifying the activity, Eye Care Leaders' incident response team immediately stopped the unauthorized access and began investigating the incident. Notably, there was no evidence that this incident involved unauthorized access to any of AOKC's patient records.

However, a lack of available forensic evidence prevented Eye Care Leaders from ruling out the possibility that some protected health information and personally identifiable information may have been exposed to the bad actor. The following categories of your information may have been stored on the myCare Integrity platform at the time of this incident: name, address, date of birth, social security number, diagnostic information, and health insurance information. However, as stated above, there was no evidence that this information was actually accessed by the bad actor.

As of this writing, AOKC has not received any reports of identity theft related to this incident.

What We Are Doing:

In response to this incident, we are mailing letters to patients whose information was stored on the myCare Integrity solution at the time of the incident. This data security incident occurred entirely within Eye Care Leaders' network environment, and there were no other remedial actions available to AOKC. We recommend that patients whose information was stored on myCare Integrity review the statements they receive from their healthcare providers. If they see any services that were not received, they should contact the provider immediately.

We value the safety of your personal information, and are therefore offering credit monitoring and identity theft protection services through IDX, a leading identity protection technology company. These services include: 12/24 months of credit monitoring and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and enroll in free IDX services by calling 1-833-909-4428 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX is available Monday through Friday 8 am to 8 pm Central Time. Please note the deadline to enroll is August 31, 2022.

IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call IDX services at 1-833-909-4428, Monday through Friday, 8 am to 8 pm Central Time.

Associated Ophthalmologists of Kansas City, P.C. values the security of your personal data, and regrets any concern or inconvenience the Eye Care Leaders data security incident may cause.

Sincerely,



Dr. James Overlease
Title



Dr. William White
Title

Associated Ophthalmologists of Kansas City, P.C.

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

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 agencies 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 violators. 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

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

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 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.