Via Email (attorneygeneral@doj.nh.gov)

February 23, 2024
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

In accordance with N.H. Rev. Stat. Ann. § 359-C:20, I am writing on behalf of Medical Management Resource Group, L.L.C. ("MMRG" or the "Company", d.b.a. American Vision Partners) to inform you about the nature and circumstances of a recent cybersecurity incident. MMRG provides administrative services to affiliated ophthalmology practices.

On November 14, 2023, MMRG detected unauthorized activity on certain parts of its network. Upon learning of this incident, MMRG promptly took steps to contain it, including isolating impacted systems. The Company also launched an investigation with the assistance of leading third-party cybersecurity firms and coordinated with law enforcement. The Company continues to take preventative actions to further safeguard its systems.

Based on the Company's investigation, MMRG determined that, in connection with the activity the Company detected on November 14, the unauthorized party obtained certain files that contained personal information about its affiliates' patients and the Company's current and former employees. The information for affected patients varied and may have included

. The information for affected current and former employees also varied and may have included

MMRG is notifying patients of this incident on behalf of the affiliated ophthalmology practices identified in Exhibit A. MMRG is notifying approximately 322 patients who are New Hampshire residents pursuant to the Health Insurance Portability and Accountability Act of 1996 Breach Notification Rule, 45 C.F.R. § 164.400-414 ("HIPAA"). Of this population, one (1) patient had their Social Security number affected.

In addition, MMRG is notifying one (1) employee who is a New Hampshire resident pursuant to N.H. Rev. Stat. Ann. § 359-C:20. MMRG will begin notifying affected current and former employees of this incident on or around Monday, February 26, 2024.

The Company also has arranged to provide individuals whose Social Security numbers were affected with identity protection and credit monitoring services for at no cost to them. Attached as Exhibit B is a sample of a notice MMRG is providing in connection with this incident.

Please do not hesitate to contact me if you have any questions.

Very truly yours,

Rose Willis, General Counsel

Enclosure

Exhibit A

CONFIDENTIAL

Exhibit B

CONFIDENTIAL

Medical Management Resource Group, L.L.C.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Medical Management Resource Group

PJHPAX00H00001
SAMPLE NAME
SAMPLE ADDRESS

February 15, 2024

PJHPAX00H0000100000101030G0500

Dear <Sample Name>,

Medical Management Resource Group, L.L.C. (d.b.a. American Vision Partners) provides administrative services to ophthalmology practices (the "Practices"). We are writing on behalf of the Practices to notify you of a cybersecurity incident that involves certain of your personal information we maintain in connection with performing services for the Practices. A list of the relevant Practices can be found in the attached Reference Guide.

On November 14, 2023, we detected unauthorized activity on certain parts of our network. Upon learning of the incident, we promptly took steps to contain it, including isolating impacted systems. We also launched an investigation with the assistance of leading third-party cybersecurity firms and coordinated with law enforcement. We continue to take preventative actions to further safeguard our systems.

On or around December 6, 2023, we determined that, in connection with the incident we detected on November 14, the unauthorized party obtained personal information associated with patients of the Practices. The information for affected patients varied and may have included your

.

We take the security of your personal information very seriously and are alerting you about this incident so that you can take steps to help protect your information. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your free credit reports and reviewing your account statements.

In addition, we have arranged to offer you identity protection and credit monitoring services for two years at no cost to you. The attached Reference Guide provides information on activation and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

We hope this information is useful to you. If you have questions regarding this incident, please call toll-free at 1-844-725-0135, Monday through Friday, 8:00 a.m. to 8:00 p.m. EST (excluding holidays).

Sincerely,

Shane Armstrong
Chief Executive Officer

Reference Guide

Ophthalmology Practices. We are providing notice on behalf of the following Practices:

We encourage affected individuals to take the following steps:

Register for Identity Protection and Credit Monitoring Services. We have arranged with TransUnion to provide you with TransUnion's Single Bureau Credit Monitoring services to help you protect your identity and your credit information for two years at no cost to you. These services provide you with alerts for two years from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. We are also providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services are provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in the Single Bureau Credit Monitoring services, please log on to **<URL>** and follow the instructions provided. When prompted, please provide the following unique code: **<UNIQUE CODE>**.

To receive the 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. Please note that when signing up for the services, you may be asked to verify personal information for your own protection to confirm your identity.

Representatives are available for 90 days from the date of this letter between the hours of 8:00 a.m. to 8:00 p.m. EST, Monday through Friday, excluding holidays. Please call us toll-free at 1-844-725-0135 if you would like further information.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected.

If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

PJHPAX00H0000100001020380000

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
http://www.doj.state.or.us

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
441 4th Street NW
Suite 1100 South
Washington, D.C. 20001
(202) 727-3400
https://oag.dc.gov

PJHPAX00H0000100001030300000