[redacted]

The Retina Group of Washington
c/o Cyberscout
[redacted]

RGW THE RETINA GROUP OF WASHINGTON

31215

[redacted]

December 22, 2023

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

0000101102G0400

P

Dear [redacted]:

The Retina Group of Washington ("RGW" or "we") places a high value on maintaining the privacy and security of patient information. Regrettably, this notice is to inform you that we were recently the victim of a cybersecurity incident (the "Incident") that resulted in the unauthorized acquisition of some of our patients' information. This notice explains the Incident, the measures we have taken in response, and the proactive steps potentially impacted individuals can take.

What Happened? On March 26, 2023, we began experiencing difficulty accessing information in some of our systems. Immediately upon becoming aware that we were experiencing a potential security incident, we took steps to secure the affected systems. We determined that we were the victim of a cybersecurity incident, initiated a privileged and confidential investigation, and reported the Incident to the Federal Bureau of Investigation. We determined that the Incident resulted in the unauthorized acquisition of some of our patients' information and, on December 8, 2023, discovered that that some of your information may have been impacted.

What Information Was Involved? Although the information involved varied among the impacted patients, the information may have included your [redacted]

What We Are Doing. Immediately upon becoming aware that we were experiencing a potential security incident, we took steps to secure the affected systems. We determined that we were the victim of a cybersecurity incident, initiated a privileged and confidential investigation, and reported the Incident to the Federal Bureau of Investigation. While we worked diligently to identify any impacted individuals, we posted a notification regarding the Incident on our website, which was available from July 7, 2023, to November 5, 2023. Although numerous procedures were previously in place, to help prevent similar incidents from happening in the future, we have implemented and are continuing to implement additional procedures and security measures to further strengthen the security of our systems.

What You Can Do. We regret that this Incident occurred and any concern it may cause. While we do not have evidence of any misuse of any patient information, we are providing you access to credit monitoring services at no charge. These services provide twenty-four (24) alerts from the enrollment date when changes occur to your TransUnion credit file. We are also providing you with proactive fraud assistance to help with any questions you might have or if you become a victim of fraud. Cyberscout will provide these services through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

[redacted]

To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted, please provide the following unique code to receive services: [redacted]

To receive the monitoring services described above, you must enroll within 90 days from the date of this letter (i.e., by March 23, 2024). The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We encourage patients to remain vigilant, review your accounts and explanation of benefits statements, and monitor your free credit reports for suspicious activity and to detect errors. This letter provides 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. Please accept our apologies that this Incident occurred.

For More Information. If you have any further questions regarding this Incident, please call our dedicated and confidential toll-free response line staffed by individuals that we have set up to respond to your specific 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 for 90 days from the date of this letter, [redacted]

Sincerely,

Dr. Steven Madreperla
President, The Retina Group of Washington

[redacted]

- OTHER IMPORTANT INFORMATION -

1. Placing a Fraud Alert.

You may 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. 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
(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. If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

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. 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

P 00001020280000

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.

5. Protecting Your Medical Information.

We have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, 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 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.

6. Attorney General Contact Information.

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. **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, www.oag.state.md.us/Consumer, 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. **New Mexico Residents**: You have rights under the federal Fair Credit Reporting Act (FCRA) which include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. **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. **Oregon Residents**: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392 **Washington D.C. Residents**: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400. There were [redacted] Rhode Island residents impacted by this incident. **All US Residents**: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.