

EyeCare Partners, LLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024



14501



February 3, 2026

Dear [REDACTED] :

EyeCare Partners, LLC (“ECP”) operates a network of eye care practices, including The Ophthalmology Group, Ophthalmology Consultants, and Ophthalmology Associates. ECP values and respects the confidentiality of the information entrusted to us and the privacy of the individuals who provide us with that information. This is why we are writing to advise you of an incident that may have involved some of your personal information. **At this time, we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft against you.** Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On or around January 28, 2025, ECP identified suspicious activity in an ECP-managed email account. Upon learning of the situation, we promptly contained the incident by securing the account to prevent further access and began an initial internal investigation into the incident. We engaged a forensic security firm to further investigate the incident and confirm the security of our computer systems and network. The forensic investigation recently concluded and has determined that an unknown, unauthorized third party temporarily accessed certain other ECP-managed email accounts between December 3, 2024, and January 28, 2025.

What Information Was Involved? Based on the findings of the investigation, we conducted a review of the information potentially accessed by the unauthorized party to determine if it contained any personal information. On November 11, 2025, we completed this review and determined that your personal information was potentially accessed. The type of information varied for each individual but may have included your name and contact information, together with your Social Security number, date of birth, drivers license/government identification number, health plan information, and limited clinical information. Your medical record and detailed clinical information, such as clinical notes, were not accessed in this incident.

What We Are Doing. In addition to the actions described above, we have also taken steps to reduce the risk of this type of incident occurring in the future, including reviewing our technical security measures and providing additional reminders to our employees about the receipt of suspicious or unexpected emails. We are also notifying you of the incident so that you can be aware and take steps to protect yourself if you feel it is appropriate to do so. Finally, although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge.

These services provide you with alerts for 24 Months 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. The Cyberscout credit monitoring and identity theft protection services is completely free to you and enrolling in this program will not hurt your credit score.

To enroll in the Cyberscout credit monitoring and identity theft protection 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]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. 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.

What You Can Do. While we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring included in this letter. If you become aware of inappropriate use of your information, we ask that you please contact the appropriate local law enforcement authorities to file a police report. You can also find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

For More Information. We value the trust you place in us to protect your privacy and take our responsibility to safeguard your personal information seriously. For further information and assistance, please call a confidential, toll-free inquiry line at [REDACTED] from 8:00 AM – 8:00 PM Eastern, Monday through Friday.

Sincerely,

Keenan R Lersch

Keenan Lersch
Chief Information Security Officer
EyeCare Partners, LLC

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Under Massachusetts law, you have the right to obtain any police report filed 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.

The District of Columbia and Massachusetts law also allow consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/ P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze 1-888-397-3742 https://www.experian.com/freeze/center.html P.O. Box 9554 Allen, TX 75013	TransUnion Security Freeze 1-800-916-8800 https://www.transunion.com/credit-freeze P.O. Box 160 Woodlyn, PA 19094
--	---	--

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.