
August 7, 2026 – Oculus Pathology (“Oculus”) has become aware of a data security incident that may have impacted information belonging to certain individuals. Oculus is not aware of any evidence to suggest that any information has been misused.

On April 1, 2026, Oculus discovered suspicious activity potentially related to an employee email account. Upon discovery, Oculus took swift action to secure its email system and network. Oculus then immediately began working with third-party computer specialists to investigate the full nature and scope of the incident. Based on the investigation, it was determined that a limited number of employee email accounts were subject to unauthorized access between March 31 and April 2, 2026. As a result, together with third-party specialists, Oculus began a comprehensive and time-consuming review of the potentially impacted email accounts to determine the type of information contained therein and to whom that information related.

While the investigation and analysis of the data potentially at risk remains ongoing, Oculus recently discovered that the affected email accounts may contain personally identifiable information (“PII”) and protected health information (“PHI”). The information contained in the affected data set may include a first and last name, in combination with one or more of the following: date of birth, Social Security number, driver’s license or state identification number, individual tax identification number, financial account number with or without access information, payment card number with or without access information, clinical information, provider name, health insurance policy number, health insurance group number, medical diagnosis information, treatment location, procedure information, medical treatment/procedure information, medical record number, Medicare number, patient ID, and/or prescription information.

At this time, Oculus is not aware of any evidence to suggest that any information has been fraudulently misused. However, in an abundance of caution, Oculus is notifying potentially impacted individuals of this incident. Although Oculus has no reason to believe any individual’s information has been or will be misused as a result of this incident, individuals are nonetheless encouraged to monitor their account statements and explanation of benefits forms for suspicious activity and to detect errors. Oculus has established a toll-free number to answer questions about the incident and to address related concerns. The number to call is 1-800-405-6108 between 8:00 am to 8:00 pm Eastern, Monday – Friday. You may also write to Oculus at Oculus at 3445 Executive Center Dr., Suite 250, Austin, TX 78731.

Oculus takes the privacy and security of the information in its care seriously, and sincerely regrets any worry or inconvenience this incident may have caused.

What steps can I take to protect my private information?

- We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. If you detect suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also report any fraudulent activity or any suspected incidents of identity theft to law enforcement.
- You may obtain a copy of your credit report at no cost from each of the three nationwide credit reporting agencies. To do so, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies appears at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.

Was my information specifically impacted?

Our investigation into the data at risk remains ongoing. Should our investigation reveal that your information was impacted, we will provide written notice directly to you. Importantly, we have no evidence to suggest that any information was subject to actual or attempted misuse as a result of this incident.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. To do so, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies is included in the notification letter and is also listed at the bottom of this page.

How do I put a fraud alert on my account?

A fraud alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and

follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is listed below.

Contact information for the three nationwide credit reporting agencies is as follows:

TransUnion	Experian	Equifax
1-800-680-7289 www.transunion.com	1-888-397-3742 www.experian.com	1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016- 2000TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348- 5069Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.