



Notice of Data Breach

Last updated: October 17, 2025

Baltimore Lab School Inc. (“Baltimore Lab School”) prioritizes the privacy and security of personal information. We were recently a victim of a security incident that resulted in the unauthorized acquisition of personally identifiable information (“PII”). This notice serves to inform individuals who applied to Baltimore School Lab, parents or legal guardians of applicants, former students of Baltimore Lab, parents or legal guardians of former students, and individuals who sought treatment through occupational therapy referrals. This notice describes the types of personal information involved, the response measures taken, and additional steps that may be considered to protect affected individuals.

On November 16, 2024, Baltimore Lab School learned of a potential IT incident after being notified by law enforcement. Ultimately, it was determined that this was a ransomware event. Upon discovery, we took immediate action, which included taking our systems offline and retaining outside cybersecurity specialists to lead our investigation. Our investigation determined that an unauthorized actor acquired certain personal information. As part of our investigation, this included retaining a data mining team to identify the data involved and to whom the data belonged. We were unable to locate all the addresses of individuals whose information may have been involved, and as a result, we are issuing this public notice to inform all potentially impacted individuals. While the information involved may vary from person to person, the types of information involved includes first and last name, in combination with one or more of the following data elements: physical or mental condition, medical diagnoses and/or treatment information, and/or school account username and password. To date, we are not aware of any reports of identity fraud or fraudulent activity involving any of this information.

Individuals who believe their information may have been involved in the incident and have not received direct notification may contact our professional assistance line, operated by Cyberscout, a TransUnion company, at 1-833-426-3205, Monday through Friday (excluding federal and major U.S. holidays), from 8:00 AM to 8:00 PM Eastern Time. As a general matter, one may remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and in order to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution, health insurance provider, or company. We have provided additional information below, “*Steps You Can Take to Help Protect Your Information*,” which contains more information about steps you can take to help protect yourself against fraud and identity theft.

Should you have any questions or concerns, please contact our professional assistance line with Cyberscout at 1-833-426-3205 Monday through Friday (excluding federal and major U.S. holidays), from 8:00 AM to 8:00 PM Eastern Time.

Sincerely,

Baltimore Lab School

Enclosure: *Steps You Can Take to Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports

You may 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. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

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

For D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and <https://doj.state.or.us/consumer-protection/>.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are no residents from Rhode Island impacted by this incident.