JacksonLewis

**Jackson Lewis P.C.**
**666 3rd Avenue, 28th Floor**
**New York, NY 10017**
**(212) 545-4000 Main**
**(212) 545-4010 Direct**
**www.jacksonlewis.com**

**VIA Email**
Office of the Attorney General
Consumer_protection@ag.idaho.gov

April 28, 2025

Re: Data Incident Notification[1]

Dear Attorney General:

On February 13, 2025, our client, Baltimore City Public Schools ("City Schools"), learned that it had experienced a criminal cybersecurity attack ("Incident") that involved the personal information of Idaho residents.

City Schools engaged an expert cybersecurity forensic investigation team to review the nature and scope of the Incident. As part of City School's extensive investigation, it worked diligently to identify personally identifiable information ("PII") that may have been subject to unauthorized acquisition as a result of the Incident. City Schools completed the review, and subsequent address lookup, on April 15, 2025.

Current and former employees, contractors, volunteers, and a limited number of students were impacted. The data elements potentially impacted for employees, contractors, and volunteers include name, Social Security number, driver's license number, passports, birth certificates, background checks, U.S. work authorizations, U.S. Naturalization certificates, and U.S. Permanent Resident cards. For students, the information included name, student ID's, dates of birth, attendance records, transcripts, maternity status, and legal records. In total, 1 Idaho resident was affected by the Incident. We are providing a courtesy notice to this office, as the impacted individual had only their name and passport information potentially impacted by the breach. City Schools notified the Idaho resident by written notice on or about April 24, 2025.

A draft copy of the notification letter is enclosed.

Since the incident, City Schools also installed additional endpoint detection and response software and reset all passwords. City Schools is reviewing its data security policies and procedures and making improvements, as needed, to minimize the risk of future incidents. Should City Schools become aware of any significant developments concerning this situation, we will

[1] Please note that by providing this letter City Schools is not agreeing to the jurisdiction of the State of Idaho, nor waiving its right to challenge jurisdiction in any subsequent actions.

inform you.

If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS, P.C.

/s/
Joseph Lazzarotti
Julia Bover
joseph.lazzarotti@jacksonlewis.com
julia.bover@jacksonlewis.com

BALTIMORE CITY
PUBLIC SCHOOLS

[First Name] [Last Name]
[Address]
[City], [State] [Zip]

Dear [First Name] [Last Name],

Baltimore City Public Schools (City Schools) is writing to notify you of a recent cybersecurity incident that may have involved some of your information. This letter provides an overview of the event and steps we are taking in response, including offering you complimentary access to credit monitoring services. Enrollment instructions for these complimentary services are included within this letter.

**What Happened?**
On February 13, 2025, Baltimore City Public Schools experienced a cybersecurity incident affecting certain IT systems within our network. We promptly notified law enforcement, conducted an initial investigation, and took steps to confirm the security of our systems. Following a thorough investigation with the guidance of law enforcement and external cybersecurity experts, we commenced a thorough review of the files to determine what information was involved and to whom the information related. We completed the review on April 15, 2025

**What information was involved?**
Our investigation confirmed your name and [data elements] were contained within files taken from our network. We are notifying you so that you may take advantage of the resources we are offering you, including complimentary access to two years of credit monitoring, identity monitoring, fraud consultation, identity theft restoration services and other support to help mitigate any potential for harm. Please see below for more information on how to enroll in these services.

**What are we doing?**
City Schools is committed to safeguarding the privacy and security of all personal information we store. We are providing this notice so you can take steps to minimize the risk your information could be used to commit identify theft or other fraud.

We have established a call center to answer your questions. The phone number and hours are at the end of this notice.

With the guidance of law enforcement and outside cybersecurity experts, we have worked diligently to determine how this incident happened, and we are taking appropriate measures to prevent a similar situation in the future. Since the incident, we have implemented a series of additional cybersecurity enhancements, including installation of endpoint detection and response software and resetting all passwords of users. We will continue to assess our procedures already in place and the results of the forensic audit for ways to defend against evolving threats.

**What can you do?**
We encourage you to take advantage of the two years of complimentary credit monitoring, identity monitoring, fraud consultation, and identity theft restoration services City Schools is providing to help mitigate any potential for harm. Please see below for more information on enrollment in these services. In addition, we have included a brief description of basic steps that can be taken to protect your identity, credit, and personal information.

As with any data incident, we encourage you to remain vigilant for incidents of fraud or misuse from any source and consider taking steps to avoid identity theft, obtain additional information, and protect personal information. If any errors or unauthorized activity are found, individuals should contact their financial institution or the appropriate service provider. A report may also be filed with law enforcement, the relevant state attorney general, and/or the Federal Trade Commission. More steps are described below.

**Enrolling in Complimentary 24-Month Credit Monitoring**
To enroll in the credit monitoring services at no charge, please visit [redacted] and enter the following activation code [redacted], to activate your membership and start monitoring your personal information. Please note the deadline to enroll is [redacted].

**Privacy Solutions** provides credit monitoring through Equifax, credit report and score access, $1 million identity theft insurance with $0 deductible, ID Restoration services, and dark web monitoring.

For additional questions, or to enroll in the complimentary credit monitoring services via phone, please contact the toll-free call center at [redacted], Monday through Friday, between 9 a.m. and 5 p.m. Eastern Time except holidays.

City Schools deeply values the trust our students, families, and staff place in us to protect the privacy and security of their information. We regret any inconvenience or concern this incident may have caused.

Sincerely,

Baltimore City Public Schools

## ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

*The following includes best practices for safeguarding your information against misuse or fraud, in addition to complimentary monitoring and protection services provided by City Schools.*

**Review Personal Account Statements and Credit Reports.** We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

| Equifax | Experian | TransUnion |
|---|---|---|
| 1-888-298-0045 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 105069 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19022 |
| www.equifax.com | www.experian.com | www.transunion.com |

**Report Suspected Fraud.** You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

**Place Fraud Alerts.** A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring, in the case of individuals impacted by this incident. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

**Place a Security Freeze.** Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

**Obtain additional information** about the steps you can take to avoid identity theft from the following entities:

**For Texas Residents:** You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General of Texas, PO Box 12548, Austin, TX 78711-2548, 800-621-0508, www.texasattorneygeneral.gov

**For District of Columbia Residents:** You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov.

**For Maryland Residents:** You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

**For New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act (FCRA). These 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 about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf

**For New York Residents:** You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

**For North Carolina Residents:** You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

**For Rhode Island Residents:** You can obtain information from the Rhode Island Attorney General about steps you can take to help prevent identity theft at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. There are approximately [redacted] Rhode Island residents potentially impacted by this incident.

**All U.S. Residents**: The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-

4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580