JacksonLewis

Jackson Lewis P.C.
666 Third Avenue
New York NY 10017-4030
(212) 545-4000 Main
(212) 972-3213 Fax
jacksonlewis.com

Direct Dial: (212) 545-4010
Email Address: Julia.bover@jacksonlewis.com

January 23, 2026

VIA EMAIL
Office of the New Hampshire Attorney General
Consumer Protection and Antitrust Bureau
DOJ-CPB@doj.nh.gov

Re: Data Incident Notification[1]

Dear Attorney General:

We are writing to notify your office that our client, Arthur Ashe Institute for Urban Health Inc. ("the Organization"), was the subject of a cyberattack ("the Incident"). The Organization immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope, the impact on its information systems, and the identities of those the Incident may have affected.

Through its extensive investigation, the Organization identified a set of files that may have been subject to unauthorized access or acquisition. It then undertook the time- and resource-intensive steps of data mining and manually reviewing the contents of those files to determine whether they contained personally identifiable information ("PII") and to identify the data subjects to whom that PII related.

On or about September 22, 2025, the Organization determined that, during the period from April 4, 2025 to May 18, 2025, the threat actor(s) may have accessed PII stored on the Organization's systems, including information related to 1 resident of New Hampshire. The categories of impacted information included names, Social Security numbers, driver's licenses, financial account information, medical information and/or health insurance information. The Organization found no evidence that this information was misused.

Out of an abundance of caution, and in accordance with applicable law, the Organization will provide notice to the affected New Hampshire residents, in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused. Additionally, the Organization has arranged for them to enroll in free credit monitoring and related services for 12 months.

The Organization treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, the Organization has taken a number of steps to further secure its systems. Specifically, it has updated passwords, implemented multi-factor authentication protocol and is reviewing its data security policies and procedures and making improvements, as needed, to minimize the risk of future incidents.

[1] Please note that the Organization is not, by providing this letter, agreeing to the jurisdiction of the State of New Hampshire, nor waiving its right to challenge jurisdiction in any subsequent action.

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

Sincerely,

JACKSON LEWIS P.C.

/s/ Julia Bover
Julia Bover, Esq.

Encl.

EXHIBIT A

001584

arthur ashe institute for urban health

P.O. Box 989728
West Sacramento, CA 95798-9728

001584

[redacted]

Enrollment Code: [redacted]
Enrollment Deadline: April 22, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

January 22, 2026

Incident Notice

Dear [redacted],

What Happened

We are writing to notify you that Arthur Ashe Institute for Urban Health Inc. ("AAIUH" or the "Organization") was the subject of a criminal cyberattack (the "Incident"). The Organization immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through its extensive investigation, AAIUH determined that the Incident resulted in unauthorized access to certain files stored on its information systems. The Organization then undertook the time- and resource-intensive steps of determining whether those files contained personally identifiable information ("PII") and to identify the data subjects to whom that PII related.

On or about September 22, 2025, AAIUH determined that, during the period from April 4, 2025, to May 18, 2025, the threat actor(s) may have accessed PII on the affected systems that related to you. The Organization has not found any evidence that your information was misused as a result of the Incident.

What Information Was Involved

The impacted files may have contained your name, along with your <<data elements>>

What We Are Doing

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we are offering identify theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-788-9712 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time, excluding holidays. Please note the deadline to enroll is April 22, 2026.

The Organization treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. As part of our ongoing commitment to cybersecurity, and in response to this Incident, we have implemented additional security enhancements, including updating passwords and implementing multi-factor authentication, and continue to regularly assess and strengthen our security measures.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

We apologize for any inconvenience this Incident may cause you. If you have additional questions, please call us at 1-833-788-9712, Monday through Friday from 9 am – 9 pm Eastern Time, excluding holidays.

Sincerely,

Arthur Ashe Institute for Urban Health Inc.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

001584

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

- Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
- You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
Consumer Fraud Division	Experian Security Assistance	Consumer Relations &
P.O. Box 740256	P.O. Box 9554	Fraud Victim Assistance
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 2000
800-685-1111	888-397-3742	Chester, PA 19016
securitymonitoring@equifax.com	businessrecordsvictimassistance@experian.com	800-916-8800.
		databreach@Transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue NW Washington, DC 20580

4. Obtain additional information about protecting your personal information from the following entities, as applicable:

For District of Columbia Residents: 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: The Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, https://oag.maryland.gov.

For New York Residents: 1) The New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) The NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

For North Carolina Residents: The North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

For Texas Residents: The Office of the Attorney General of Texas, PO Box 12548, Austin, TX 78711-2548, 800-621-0508, www.texasattorneygeneral.gov.