

Notice of Security Incident

Westchester Institute for Human Development, Inc.
Notice of Data Security Incident

The privacy and security of the personal information we maintain is of the utmost importance to Westchester Institute for Human Development, Inc. ("WIHD").

On or about April 8, 2026, we experienced unauthorized access to our email environment. Upon detecting the unauthorized activity, we immediately took steps to contain the incident and commenced an immediate and thorough investigation. As part of our investigation, we engaged cybersecurity experts to identify what personal information, if any, was involved.

After an extensive forensic investigation, we discovered that between March 23, 2026 and April 14, 2026, an unauthorized user may have accessed some of our files. We conducted a thorough manual review of the potentially impacted data, and on July 29, 2026, we determined that the files may have contained some personal information, including name, Social Security number, driver's license number, date of birth, date of medical service, health insurance policy number, provider information, medical condition, diagnosis, or treatment information, medical record number, Medicare or Medicaid number, financial account information, patient account number, full face photo, and referral information. The information varies by person. Only a limited number of individuals had their information impacted and not all patients had their information impacted.

We have no evidence of any identity theft related to this incident. However, out of an abundance of caution, we remind individuals to remain vigilant in reviewing financial account statements on a regular basis for any fraudulent activity.

We are committed to maintaining the privacy of personal information in our possession and have taken significant precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of the personal information we maintain.

Individuals who have questions or need additional information regarding this incident may reach out to **1-800-405-6108** between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Other Important Information

copy of your credit report by calling **1-877-322-8228**, visiting www.annualcreditreport.com, 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 access the request form at <https://www.annualcreditreport.com/index.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below.

<i>Equifax</i>	<i>Experian</i>	<i>TransUnion</i>
P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

2. Placing a Fraud Alert on Your Credit File

We recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>.

<i>Equifax</i>	<i>Experian</i>	<i>TransUnion</i>
P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289

3. Placing a Security Freeze on Your Credit File

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. 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. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

<i>Equifax Security Freeze</i>	<i>Experian Security Freeze</i>	<i>TransUnion Security Freeze</i>
--------------------------------	---------------------------------	-----------------------------------

(888) 298-0045	(888) 397-3742	(888) 909-8872
----------------	----------------	----------------

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

4. Protecting Medical Information

As a general matter, the following practices can help deter, detect, and protect from medical identity theft. For more information visit consumer.ftc.gov/articles/what-know-about-medical-identity-theft. Only share health insurance cards with health care providers and other family members who are covered under the insurance plan or who help with medical care. Review the "explanation of benefits statement" which is provided by the health insurance company. Follow up with the insurance company or care provider for any items not recognized. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date. Ask the insurance company for a current year-to-date report of all services paid for the impacted individual as a beneficiary. Follow up with the insurance company or the care provider for any items not recognized.

5. Additional Helpful Resources

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

Sign up for updates!

* Email

First Name

Last Name

By submitting this form, you are consenting to receive marketing emails from: Westchester Institute for Human Development, Cedarwood Hall, Valhalla, NY, 10595, US, <http://www.wihd.org>. You can revoke your consent to receive emails at any time by using the [SafeUnsubscribe®](#) link, found at the bottom of every email. **Emails are serviced by Constant Contact.**

Sign up!

Cedarwood Hall
Valhalla, NY 10595
Phone: 914-493-8150
Clinic: 914-493-8148
Email: info@WIHD.org

> [Contact](#)

> [Non-Discrimination Notice & Language Assistance Services](#)

> [Website Privacy Policy](#)

> [Notice of Privacy Practices](#)

> [Staff Resources](#)

Search...

Q

