Hitachi Vantara, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

HITACHI

[redacted]

November 19, 2026

Notice of Data Breach

Dear [redacted]

We are reaching out to provide the important conclusions reached in our forensic investigation of the data security incident by an unauthorized third party that occurred on Saturday, April 26, 2025. Below, please find information regarding the data that was involved in the incident and the steps that can be taken to protect personal information going forward.

What Happened?
On April 26, 2025, we detected suspicious activity on Hitachi Vantara's servers. From the moment we detected suspicious activity, we took action, reporting the incident to law enforcement, launching our incident response protocols, and engaging third-party experts to support our investigation, remediation, and file review processes.

As initially reported to employees on May 20, 2025, the unauthorized third party responsible for this incident accessed files within Hitachi Vantara servers that contained personal information pertaining employees of Hitachi Vantara, Hitachi Vantara Manufacturing, Hitachi Digital Services, Hitachi Digital, and Pentaho. As soon as it was feasible to, we engaged third-party experts to decrypt the accessed files and complete a thorough review of the information within them. This notification was not delayed at the request of law enforcement.

What Information Was Involved?
Upon the completion of the review on June 29, 2026, we can now report that, for you specifically, the information involved included Date of Birth, Employee Identification Number, home address, LDAP, Marital Status, Personal Phone, Race/Ethnic Origin, Salary Information and Social Security Number.

To date, we have no indication that the unlawfully accessed information has been sold, disseminated, or otherwise misused and we are not currently aware of any reports of fraud.

What Are We Doing?
We have activated enhanced detection and monitoring tools across our environment. No new unauthorized activity has been detected in our network since April 27, 2025. We continue to rely on and improve our access management tools for security.

We take seriously our responsibility to safeguard the privacy of our employees' information. We are continuing to work with third-party experts to enhance the security of our systems and the data entrusted to us. Please know that, as part of our incident response and our activities since this incident, **we have taken and will continue to take any and all possible steps to protect your personal data.**

What Can You Do?
It is always a good practice to remain vigilant for incidents of fraud and identify theft. Generally, we suggest that employees review financial account statements and monitor credit reports for any suspicious or unusual activity. Immediately report suspicious activity or incidents of identity theft to the three nationwide credit bureaus: Equifax, Experian, or Transunion, the police, and the Federal Trade Commission (FTC), as appropriate.

U.S. employees may access free credit monitoring and fraud resolution services from Experian Consumer Direct as part of Hitachi's existing U.S. employee benefits. The benefit includes: a credit monitoring from all three bureaus; access to your Experian credit report; CyberAgent® Dark Web Monitoring, $1M identity theft insurance and full-service identity restoration. If not currently enrolled, employees may visit https://benefits.hitachivantara.com/perks-and-family/identity-theft-and-credit-monitoring/ for more information or they may contact the Hitachi Benefits Pool at 844-318-3274 to obtain instructions and an activation code to enroll in Experian IdentityWorks.

We recommend the review of the "Additional Important Information" section enclosed, which contains important steps that can be taken to protect personal information, including recommendations by the FTC regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file.

For More Information
We recognize that there may be questions.

For questions about Hitachi's credit monitoring and fraud resolution services, contact the Hitachi Benefits Pool at 844-318-3274 or visit https://benefits.hitachivantara.com/perks-and-family/identity-theft-and-credit-monitoring/. Note that the Hitachi Benefits Pool will not be able to answer questions about the incident.

For questions regarding the incident, representatives are available for 90 days from the date of this letter, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-319-8595.

We regret any inconvenience this incident may have caused. Thank you for your patience during our investigation.

The Hitachi Digital Data Privacy Office

Additional Important Information

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.
For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission (FTC).
For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. 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, visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the FTC listed below.
For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There were four Rhode Island residents notified in this incident.

DC Attorney General	**Maryland Office of Attorney General**	**New York Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
400 6th Street NW	200 St. Paul Pl	120 Broadway, 3rd Fl	9001 Mail Service Ctr	150 South Main St
Washington, DC 20001	Baltimore, MD 21202	New York, NY 10271	Raleigh, NC 27699	Providence RI 02903
1-202-727-3400	1-888-743-0023	1-800-771-7755	1-877-566-7226	1-401-274-4400
www.oag.dc.gov	https://www.marylandattorneygeneral.gov/	www.ag.ny.gov	https://ncdoj.gov/	www.riag.ri.gov

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.identitytheft.gov

Massachusetts and Rhode Island residents: You have the right to obtain or file a police report.
For residents of all states:
You may obtain a free copy of your credit report whether or not you suspect any unauthorized activity on your account from each of the three nationwide credit reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.
Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.
Monitoring: Always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity. Immediately report any suspicious activity or incidents of identity theft.
Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze, make a request to each consumer reporting agency via their websites below or via mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, be prepared to provide name, address for the past two years, date of birth, Social Security number, proof of identity, and proof of address to the credit reporting company. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348-5788	Allen, TX 75013-9544	Woodlyn, PA 19094
www.equifax.com/personal/credit-report-services/credit-freeze/	http://www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
1-866-478-0027	1-888-397-3742	1-800-916-8800