Wendy F. Hensel
President

UNIVERSITY of HAWAIʻI®
Ke Kulanui o Hawaiʻi

DEPT. COMM. NO. 386

May 4, 2026

The Honorable Ronald D. Kouchi,
President and Members of the Senate
Thirty-Third State Legislature
Honolulu, Hawaiʻi 96813

The Honorable Nadine K. Nakamura, Speaker
and Members of the House of Representatives
Thirty-Third State Legislature
Honolulu, Hawaiʻi 96813

Dear President Kouchi, Speaker Nakamura, and Members of the Legislature:

For your information and consideration, the University of Hawaiʻi is transmitting a copy of the Report on Data Exposure at the University of Hawaiʻi at Mānoa – College of Education (Section 487N-4, Hawaiʻi Revised Statutes) as requested by the Legislature.

In accordance with Section 93-16, Hawaiʻi Revised Statutes, this report may be viewed electronically at: https://www.hawaii.edu/govrel/docs/reports/2026/hrs487n-4_2026_college-of-education-report_508.pdf.

Should you have any questions about this report, please do not hesitate to contact Stephanie Kim at (808) 956-4250, or via e-mail at scskim@hawaii.edu.

Sincerely,

Wendy F. Hensel
President

Enclosure

2444 Dole Street, Bachman Hall
Honolulu, Hawaiʻi 96822
Telephone: (808) 956-8207
Fax: (808) 956-5286
An Equal Opportunity Institution

UNIVERSITY OF HAWAIʻI SYSTEM REPORT

REPORT TO THE 2026 LEGISLATURE

Report on Data Exposure at the
University of Hawaiʻi at Mānoa – College of Education

HRS 487N-4

May 2026

Subject: Report to the Legislature on the Data Exposure at the University of Hawai'i at Manoa – College of Education

Discovery of Data Exposure:	April 2026
Location of the Data Exposure:	University of Hawai'i at Manoa – College of Education
Nature of Exposure:	Malware from a third-party site

Incident Description:

On or about April 14, 2026, the University determined that a data security incident may have involved the names and Social Security numbers of two individuals. The incident was identified through information security monitoring on a university-owned laptop assigned to a College of Education faculty member. The College of Education and System Information Technology Services promptly investigated and determined that the device had been compromised after interaction with a third-party website. There is no evidence that the College or the University was intentionally targeted.

There is no indication that the incident extended beyond the single device or affected other University systems.

A review of files on the device identified documents containing the names and Social Security numbers of two individuals. Since the University cannot confirm with certainty whether that data was taken, viewed, copied, or removed, the University will notify the two individuals and offer credit monitoring and identity theft monitoring services through Experian. Attachment A is a sample of the notification letter.

Remediation:

- Removed files containing personally identifiable information from the affected device.
- Issued a replacement computer to the affected faculty member with enhanced security features installed on it.
- Reset the faculty member's passwords across university systems.
- Reviewed University systems for indicators of unauthorized access.
- The College of Education is continuing to increase security on its devices.
- The College of Education is conducting workshops on data retention policies, secure deletion of files, data governance classification, and proper data governance practices.
- The College of Education launched a recurring informational email campaign to educate faculty and staff on emerging cybersecurity threats, protective measures, and other topics to increase awareness.

College of Education
Office of the Dean

UNIVERSITY of HAWAI'I® MĀNOA

ATTACHMENT A

[Date]

(First Name) (Last Name)
(Address Line 1)
(Address Line 2)

RE: Notice of Data Exposure

Dear (First Name) (Last Name),

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On April 14, 2026, a computer at the University of Hawai'i at Mānoa College of Education was found to be compromised with malware.

What information was involved?

The compromised laptop contained a file with your name and Social Security number. And while there is no clear evidence that the attackers viewed or removed any of the files, we are notifying you of the possible exposure of your information.

What we are doing.

When it was discovered that the computer was compromised, it was taken offline. Additionally, all files containing Personal Identifiable Information (PII) were securely deleted. We are implementing additional security measures to detect and prevent similar attacks, such as additional monitoring and security architecture review.

To help protect your identity, we are offering to reimburse you for a one-year membership with Experian. We have authorized reimbursement for the Premium Plan, up to an amount of $24.99 per month. This service provides identity theft detection and resolution of identity theft.

If you wish to enroll in this monitoring service and set up your monthly reimbursement, please contact the College of Education at sheryl@hawaii.edu or (808) 956-4279. We will provide you with the necessary steps to facilitate the setup and ensure your protection is active.

1776 University Avenue
Everly Hall, Room 128
Honolulu, Hawai'i 96822
Tel: (808) 956-7703 • Fax: (808) 956-3106
An Equal Employment Opportunity Institution

What you can do.

We also urge you to carefully monitor your credit card statements and to take heightened protective measures including:

- Obtain and carefully review your credit reports. You can order free credit reports from all three credit agencies at https://www.annualcreditreport.com
- Review your bank and credit card statements regularly and look for unusual or suspicious activities
- Contact appropriate financial institutions immediately if you notice any irregularity in your credit report or any account. If your accounts or identity have been compromised, you may take immediate actions such as requesting refunds, closing accounts, placing your credit reports in a state of "fraud alert" or "freeze", and filling a police report.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call Sheryl Tashima at (808) 956-4279 or email sheryl@hawaii.edu, Monday through Friday, from 9:00 a.m. to 3:00 p.m. Hawai‘i Time.

We apologize for this incident and regret any inconvenience it may have caused you. Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security.

Sincerely,

Nathan M. Murata
Dean and Professor

Attachment: Additional Resources

ADDITIONAL RESOURCES

Nationwide Credit Reporting Agencies

Contact information for the three nationwide credit reporting agencies is:

Equifax
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-685-1111

Experian
P.O. Box 2104
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
www.transunion.com
1-888-909-8872

Free Credit Reports. You should remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports for unauthorized activity. Federal law gives you the right to obtain a free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. The three nationwide credit reporting agencies also currently allow consumers to check their credit report from each agency once a week for free through www.annualcreditreport.com. To order your free credit reports, visit www.annualcreditreport.com, call toll free at 1-877-322-8228, or mail a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You may place a fraud alert on your credit file if you are, or suspect you may be, affected by identity theft. A fraud alert tells businesses to check with you before opening a new credit account in your name. An initial fraud alert lasts one year and is free. To place an initial fraud alert, contact one of the three nationwide credit reporting agencies. The agency you contact must notify the other two agencies to place the fraud alert on your credit report.

Security Freeze. You may place a security freeze on your credit report. A security freeze helps prevent new credit accounts from being opened in your name by restricting access to your credit report. There is no cost to place or lift a security freeze, and a security freeze does not affect your credit score. A security freeze remains in place until you lift it. To place a security freeze, you must contact all three nationwide credit reporting agencies: Equifax, Experian, and TransUnion. If you later need to apply for credit, rent housing, buy insurance, or complete

another transaction that requires a credit check, you may temporarily lift the freeze and reinstate it after the credit check is complete.

Federal Trade Commission. If you believe your information has been misused, you may report identity theft to the Federal Trade Commission at www.IdentityTheft.gov or by calling 1-877-ID-THEFT (1-877-438-4338). The FTC provides recovery guidance and a personalized recovery plan for individuals who report identity theft.

Hawaii Law Enforcement and State Resources. If you believe you are a victim of identity theft, you may file a police report with your local police department. The Hawaii Department of the Attorney General advises identity theft victims to close any financial accounts that have been tampered with or established fraudulently, file a police report to help with creditors who may request proof of the crime, obtain the police report number and a copy of the report if possible, place a one-year fraud alert on their credit file, and review credit reports carefully.

Additional Steps You Can Take. You should review your bank, credit card, and other financial account statements regularly and report any suspicious activity to the applicable financial institution. If you identify unauthorized activity, consider changing account passwords, closing affected accounts, placing a fraud alert or security freeze, filing a police report, and reporting identity theft to the FTC at www.IdentityTheft.gov.