UNIVERSITY OF HAWAI'I
CANCER CENTER

NOTICE OF DATA INCIDENT

This is notification by the University of Hawai'i Cancer Center ("UHCC") of an event that may have involved Social Security numbers (SSNs), driver's license (DL) numbers, names, addresses, and, in some cases research data for certain individuals defined below. This notification provides affected individuals details of the incident, our response, and resources available to help protect individuals' information, should it be necessary to do so. Individuals who participated in the Multiethnic Cohort Study (MEC Study) were mailed notifications on February 23, 2026, but all others whose SSNs and/or DL numbers may have been affected by this incident are being notified via email where an email address could be located and/or through publication.

What happened. On or about August 31, 2025, UHCC identified a cybersecurity incident isolated to several specific systems that support its Epidemiology Division. There has been no impact on clinical operations or patient care at UHCC. No student records were impacted.

After quickly identifying that a threat actor (TA) had accessed certain research files, UHCC promptly disconnected affected systems and took steps to terminate the TA's unauthorized access and mitigate risk to data. Experts were immediately engaged to investigate and determine the nature and scope of the incident. Keeping law enforcement and external stakeholders informed, UHCC worked with an external team of cybersecurity experts to obtain a means to unlock its systems and to secure and affirm the destruction of the data by the TA.

Due to the extensiveness of the encryption, it took some time to restore the affected systems and assess the impact to data. Once the affected systems became accessible, UHCC promptly began identifying potentially impacted files that may have contained personal information.

There is no evidence that the personal information was published, disseminated, or misused. Nonetheless, UHCC is notifying those whose information was in the impacted files so they may take steps to protect themselves, as necessary.

What information was involved. During the investigation, it was determined that an unauthorized third party gained access to and had the opportunity to exfiltrate a subset of research files used for certain epidemiology studies and recruitment efforts on the servers supporting epidemiology research operations at UHCC. This included the following files containing personal information (SSNs and/or DLs in combination with names):

1. Two files containing names in combination with SSNs: the first, containing DL numbers, was collected in the year 2000 from the State Department of Transportation; the second, containing voter registration information, was collected in the year 1998 from the City & County of Honolulu. At that time, DL numbers in Hawai'i were typically based on SSNs, and City and County of Honolulu voter registration information also often contained SSNs.
2. Files for study participants in the long-running Multi-Ethnic Cohort (MEC) Study (recruitment for participants in Hawai'i and Los Angeles, California from 1993-1996) and three other epidemiological studies of diet and cancer focusing on colorectal adenomas (recruitment for participants 1995-2007) and colon cancer (recruitment for participants 1994-2005), which also had SSNs and/or DL numbers in combination with names. They may also have contained questionnaires and other study information on participant health, as well as information pulled from national and state public health registries.
3. Two files that contain SSNs in combination with names collected from national and state public health registries as part of epidemiology research and study recruitment efforts. One file was closed to new names in 1999, and the other in the mid-2000s. The impacted files may also have contained research registry information about individuals' health.

What are we doing in response. In addition to launching a forensic investigation into this incident and notifying individuals, we enhanced existing security of our systems by resetting passwords and implementing additional technical and organizational protection measures. Our security team and third-party cyber professionals continue to monitor our systems for any unusual activity.

What can you do. If you believe you may have been affected by this incident, please contact (844) 443-0842 (hours below) for more information about resources we are offering to you. To help protect yourself, we recommend remaining vigilant by reviewing and monitoring your financial account statements, and free credit reports for suspicious activity. We have included below some additional steps that you can take to protect yourself, as you deem appropriate. While we have no evidence that any personal information has been used inappropriately, we recommend you take precautions. **If your information was involved, we are offering you 12 months of *free* credit monitoring and $1 million in identity theft insurance - to give you peace of mind. *You must activate the free product by the activation date in order for it to be effective. Please call the number above to learn how to enroll in the credit monitoring services.***

For more information about this incident, starting Monday, March 2, please call toll free (844) 443-0842 during the following hours.

- Monday to Friday, 8:30 a.m. to 9 p.m. Central Time (excluding holidays)
    - March 2-6, 2026, 4:30 a.m. to 5 p.m., Hawai‘i Standard Time
    - Starting March 9 (due to daylight savings time), 3:30 a.m. to 4 p.m. Hawai‘i Standard Time

We continue to take steps to enhance our security measures to help prevent something like this from happening in the future.

Sincerely,

Naoto T. Ueno
Director, University of Hawai‘i Cancer Center

STEPS YOU CAN TAKE

➢ **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

➢ **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

➢ **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

➢ **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 1-877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

➢ **LAW ENFORCEMENT INVOLVEMENT:** Though law enforcement was notified of the incident, this notification

has not been delayed as a result of a law enforcement investigation.

- **FAIR CREDIT REPORTING ACT (FCRA):** Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore/ or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. 10) You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. 11) You may seek damages from violators. 12) Identity theft victims and active-duty military personnel have additional rights.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to https://www.experian.com/fraud/center.html. Federal Trade Commission also provides information at https://consumer.ftc.gov/features/identity-theft FTC hotline is 1-877-438-4338; TTY: 1-866-653-4261 or write to the FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.