UNIVERSITY OF HAWAIʻI SYSTEM REPORT

REPORT TO THE 2023 LEGISLATURE

Report on Data Exposure at the UH Maui College

HRS 487N-4

April 2023

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

Discovery of Data Exposure:	February 2023
Location of the Data Exposure:	University of Hawai'i Maui College (UHMC)
Nature of the Exposure:	Unauthorized access to IT network

Incident Description:
In mid-February 2023, UHMC learned of a security incident indicating unauthorized access to the the UHMC network. Immediate actions were taken to terminate the unauthorized access and mitigate risk to data. Experts were immediately engaged to investigate and determine the nature and scope of the incident. The incident was reported to law enforcement. The intrusion was isolated to the UHMC network and did not impact other networks in the University of Hawai'i System. The event also did not affect UHMC's operations.

During the course of the investigation, it was determined that an unauthorized 3rd party may have accessed and possibly exfiltrated a subset of the files on the UHMC network, which had been protected by a firewall and other safeguards. UHMC immediately began to scan and manually review the affected files to determine if sensitive information was stored in the files and to determine how many individuals may have been affected. Out of an abundance of caution, notification letters are being sent out to approximately 10,500 individuals, which will include an offer of credit monitoring and identity theft protection services through Experian. Attachment A is a sample of the notification letter that is being sent by UHMC on or about April 6, 2023.

Remediation:
- Installed monitoring software with 24/7 monitoring of endpoints.
- Retained third party experts to contain and remediate the event.
- Created replacement accounts for any compromised user accounts.
- Reset passwords.
- Rebuilding network utilizing a new firewall with additional security controls to ensure that attack path is closed.
- Rebuilding compromised systems to ensure that all malware has been eliminated and create new accounts/passwords to ensure that attackers no longer have access and move these "clean" systems into the new network.
- Rebuilding and hardening security features for all servers and appropriately deleting any unneeded files.
- Reviewing all security configurations and implementing recommendations made by 3rd party experts.
- Conducting a 3rd party external assessment to validate the security controls of the new network, systems, and servers.

ATTACHMENT A

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>> <<Country>>

Re: Notice of Security Incident

Dear <<Name1>>:

On behalf of University of Hawai‘i Maui College ("UHMC"), I am writing to notify you of a recent incident that may have involved some of your personal information.

What happened? On or about February 15, 2023, UHMC learned of a possible data security incident that may have involved the potential compromise of certain files in UHMC's IT environment. Immediately upon learning of the incident, experts were engaged to investigate and evaluate the nature and scope of the incident. We also reported the incident to law enforcement.

What information was involved? On or about February 23, 2023, UHMC was advised that an unauthorized third party may have accessed and/or potentially exfiltrated certain limited files from the UHMC network. In response, UHMC undertook an extensive and arduous document review process (which involved the programmatic searching and hand-reviewing of individual documents) in order to identify individuals who potentially needed to be notified of this incident. Through these efforts, UHMC recently determined that the impacted files may have contained some of your personal information, such as your name and social security number.

What are we doing and what can you do? In response to this incident, we have taken remediation measures, implemented several security enhancements, further secured our network, and will continue to evaluate additional measures we can take to harden our defenses. Importantly, the incident did not impact UHMC's operations.

While we are not aware of any instances of fraud at this time, we recommend you consider taking precautions, and remain vigilant against incidents of identity theft and fraud. As a precaution, UHMC encourages you to review your account statements and to monitor your personal information for suspicious activity and to detect errors.

Also, for your peace of mind, we are offering you 12 months of *free* credit monitoring and identity theft protection through Experian. ***This product is being offered at no cost to you but you must activate the free product by the activation date in order for it to be effective. The activation instructions are included with this letter.*** We also have included some additional steps you can take to protect yourself, as you deem appropriate.

For more information about this incident, please call 888-493-2172 between the hours of 6 AM and 6 PM Pacific Time, Monday - Friday (excluding major U.S. holidays).

We understand the concern that this issue may raise for our students, employees and other members of our community. UHMC takes seriously our responsibility to protect the data entrusted to us. Even before this incident, we worked diligently to constantly evaluate our security posture and enhance the safeguards in our network. We are fully committed to protecting your personal information and sincerely apologize for any inconvenience or concern this may have caused.

Sincerely,

Dr. Lui Hokoana
Chancellor

STEPS YOU CAN TAKE

Below is information on steps you can take to protect yourself personally, if you feel that is appropriate under the circumstances.

➢ **ACTIVATE Your FREE Experian IdentityWorks Product NOW in Three Easy Steps.** To help protect your identity, we are offering you a **complimentary 12 month membership** of Experian's IdentityWorks product. This product helps detect possible future misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks Alert is completely free to you and enrolling in this program will not hurt your credit score.

1. ENSURE You Enroll By: **<<Enrollment Deadline>>** (Your code will not work after this date.)
2. VISIT the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
3. PROVIDE Your Activation Code: **<<Activation Code>>**

If you have questions about the IdentityWorks or need an alternative to enrolling online, **please call 877-288-8057** and provide engagement number **<<Engagement Number>>.** A credit card is not required for enrollment. Once your IdentityWorks membership is activated, you will receive the following features:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Restoration Agents are immediately available to help address credit/non-credit related fraud.
- **$1 Million Identity Theft Insurance:[2]** Provides coverage for certain costs and unauthorized electronic fund transfers.

You must activate your membership by the Enrollment Date (noted above) by enrolling at https://www.experianidworks.com/3bcredit or calling 877-288-8057 to register your activation code above in order for this service to be activated. Once your enrollment in IdentityWorks is complete, carefully review your credit report for inaccurate or suspicious items. If you have any questions about IdentityWorks, need help understanding something on your credit report, or suspect that an item on your credit report may be fraudulent, please contact Experian's customer team at 877-288-8057.

Additional Steps You May Wish to Take:

➢ **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your personal 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. A 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 the freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 ACCOUNT / CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your bank account and/or personal credit file. An initial credit file fraud alert is a 1-year alert that is placed for free 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.** Always carefully review your credit reports, healthcare provider billing statements, 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 the same password is used over multiple online accounts. If there are suspicious or fraudulent charges to your insurance statements, healthcare provider billing statements, credit report, credit card or bank accounts, immediately provide details 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 877-322-8228 to obtain 1 free copy of your credit report from each of the 3 credit reporting agencies 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 3 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

➢ **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it. Notification of this incident 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 http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for additional information. The Federal Trade Commission (FTC) also provides information at www.ftc.gov/idtheft. The FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

➢ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM YOUR STATE ATTORNEY GENERAL.**

- ***District of Columbia:*** *You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, databreach@dc.gov, www.oag.dc.gov.*
- ***Maryland:*** *You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662; www.oag.state.md.us; Consumer Hotline 1-410-528-8662, or consumer@oag.state.md.us.*
- ***Massachusetts:*** *Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.*
- ***New York:*** *You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.*
- ***North Carolina:*** *You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov.*