



UNIVERSITY
of HAWAII*
SYSTEM

David Lassner
President
DEPT. COMM. NO. 416

February 10, 2020

The Honorable Ronald D. Kouchi,
President and Members of the Senate
Thirtieth State Legislature
Honolulu, Hawai'i 96813

The Honorable Scott Saiki, Speaker
and Members of the House of Representatives
Thirtieth State Legislature
Honolulu, Hawai'i 96813

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

For your information and consideration, the University of Hawai'i is transmitting one copy of the Report on Data Exposure at the University of Hawai'i at Mānoa School of Nursing and Dental Hygiene (Section 487N-4, Hawai'i Revised Statutes) as requested by the Legislature.

In accordance with Section 93-16, Hawai'i Revised Statutes, this report may be viewed electronically at: <https://www.hawaii.edu/offices/government-relations/2020-legislative-reports/>.

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

Sincerely,

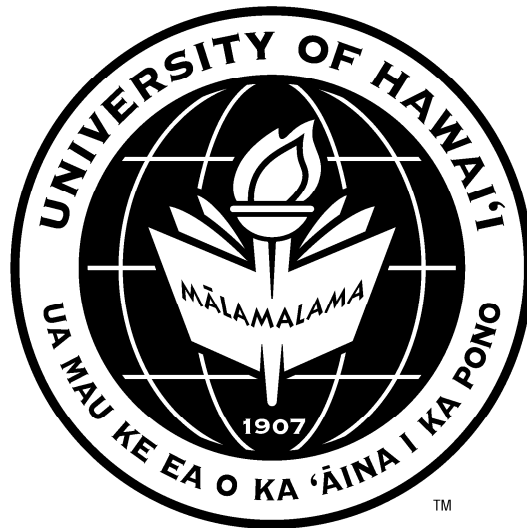
A handwritten signature in black ink that reads 'David Lassner'.

David Lassner
President

Enclosure

2444 Dole Street, Bachman Hall
Honolulu, Hawai'i 96822
Telephone: (808) 956-8207
Fax: (808) 956-5286
An Equal Opportunity/Affirmative Action Institution

UNIVERSITY OF HAWAI‘I SYSTEM REPORT



REPORT TO THE 2020 LEGISLATURE

Report on Data Exposure at the
University of Hawai'i at Mānoa School of Nursing and Dental Hygiene

HRS 487N-4

February 2020

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

Discovery of Data Exposure: November 2019
Location of Data Exposure: University of Hawai'i at Mānoa
Nature of Data Exposure: Files containing sensitive information discovered while investigating a Ransomware incident

Incident Description:

In November 2019, the School of Nursing and Dental Hygiene's (SONDH) servers were found to be compromised with ransomware. The type of attack used by the attacker was a low and slow brute force attack which is difficult to detect. In these types of attacks, the attacker systematically attempts to login with different passwords until they are successful. The attempts are spread out over a long period of time specifically to avoid detection. After gaining access to the servers, the attackers launched a ransomware attack. Upon detection of the compromise, all servers were immediately taken offline.

While the servers were protected by a firewall, the attackers were able to evade detection and compromise login credentials to gain access to the servers. The compromised servers contained files with names and Social Security Numbers. There was no clear evidence that the attackers viewed or removed any files.

Approximately 498 individuals have been identified. Out of an abundance of caution, notification letters are being sent out and all potentially affected individuals are being provided two (2) years of credit monitoring services (Attachment A).

Remediation steps taken by SONDH:

- Rebuild compromised systems to ensure that all malware has been eliminated and create new accounts/passwords to ensure that attackers no longer have access.
- Securely remove any sensitive information if not required for business operations.
- Ensure that all sensitive information is encrypted.
- Harden servers by:
 - Ensure that all accounts have strong passwords and use multi-factor authentication wherever possible
 - Perform regular patching
 - Set up least privilege accounts and access control lists to ensure that only authorized users have system administrator access
 - Ensure that security logs are closely monitored to better detect and respond to incidents.
- Redoubling efforts on education and training regarding proper handling of sensitive information at the departmental level.
- Check individual systems for indicators of compromise to look for any other undetected backdoors.
- Review network architecture and security controls and increase monitoring to attempt to better identify these types of attacks.



UNIVERSITY
of HAWAII®
MĀNOA

February 10, 2020

(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 November 25, 2019, the University of Hawai'i at Mānoa School of Nursing and Dental Hygiene's servers were found to be compromised with ransomware. The attackers systematically attempted to login with different passwords until they were successful. Their attempts were spread out over a long period of time to avoid detection.

What information was involved?

The compromised servers contained files with names and Social Security numbers. 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 servers were compromised, the affected servers were immediately taken offline and have subsequently been decommissioned permanently. All files containing PII (Personal Identifiable Information) have been removed in accordance with the US Department of Defense deletion standard (DOD 5220.22-M) and will no longer be housed on any servers in the future. We are implementing additional security measures in an attempt to detect and prevent similar attacks, such as additional monitoring and security architecture review.

To help protect your identity, we are offering two-year membership with Experian's® IdentityWorksSM at no cost to you. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: April 30, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code: (unique code to be inserted)**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 (toll-free) by April 30, 2020. Be prepared to provide engagement number **DB17579** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332 (toll-free). If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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.

If you are a student, the U.S. Dept. of Education Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at:

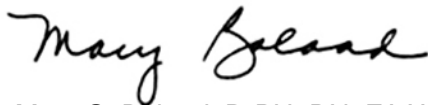
- <http://www.ed.gov/about/offices/list/oig/misused/idtheft.html>;
- <http://www.ed.gov/about/offices/list/oig/misused/victim.html>.

For more information.

If you have questions, please call 808-956-8522, Monday through Friday, from 8:00 a.m. to 5:00 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,

A handwritten signature in black ink that reads "Mary Boland". The signature is written in a cursive, flowing style.

Mary G. Boland, DrPH, RN, FAAN
Dean and Professor

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

- **For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability 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 on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

- **For Massachusetts residents:** The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is \$5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's Office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**. Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

- **For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.
- **For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

- **For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.
- **For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.
- **For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.