



UNIVERSITY
of HAWAII
SYSTEM

David Lassner
President

DEPT. COMM. NO. 45

November 15, 2017

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

The Honorable Scott Saiki, Speaker
and Members of the House of
Representatives
Twenty-Ninth 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 a copy of the Report to the Legislature on the Security Breach at the University of Hawai'i (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: <http://www.hawaii.edu/offices/government-relations/2017-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, appearing to read "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 2017 LEGISLATURE

Report on Security Breach
at the University of Hawai'i
October 2017

HRS 487N-4

Subject: Report to the Legislature on Data Exposure at the University of Hawaii

Discovery of Data Exposure: October 2017
Location of Data Exposure: University of Hawai'i
Nature of Data Exposure: Files containing sensitive information discovered while investigating a Business Email Compromise (BEC)

Incident Description:

In October 2017, while investigating an email compromise, network devices on the University of Hawai'i (UH) network were found to contain sensitive information. At this time, UH cannot confirm that any of the sensitive information was taken or that it was misused.

It is important to note that these types of attacks are extremely difficult to detect and to protect against. The network was protected by a firewall but the attackers were able to circumvent security controls and compromise login credentials to gain access to the network.

UH is in consultation with federal law enforcement agencies and is continuing its investigation. Due to the sensitivities of the investigation, more comprehensive details will be supplied at a later date when doing so does not impede the investigations. Approximately 2400 individuals have been identified. Notification letters are being sent out and all potentially affected individuals are being provided one (1) year of credit monitoring services (Attachment A).

Remediation:

Update UH Policy to ALWAYS require encryption of sensitive information at rest regardless of the security of the network, server or device.

Redoubling efforts on education and training regarding proper handling of sensitive information at the departmental level.

Securely remove any sensitive information if not required for business operations.

Rebuilding compromised systems to ensure that all backdoors into the network have been eliminated.

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 identify these types of sophisticated attacks.



UNIVERSITY
of HAWAII®
SYSTEM

Garret T. Yoshimi
Vice President for Information Technology
and Chief Information Officer

ATTACHMENT A

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<ClientDef1(Care of FirstName LastName)>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

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?

In October 2017, while investigating an email compromise, network devices that contain sensitive information on a University of Hawai'i (UH) campus were discovered to have been potentially compromised.

It is important to note that the type of attack utilized is extremely difficult to detect and to protect against. The network was protected by a firewall but the attackers were able to circumvent security controls and compromise login credentials to gain access to the network. UH is in consultation with federal law enforcement agencies as part of a continuing investigation.

What information was involved?

At this time, we cannot confirm that any sensitive personal information was stolen or misused. It is with an abundance of caution that we are providing you with this notice. The sensitive information, which was potentially exposed, included your name and Social Security number. However, others may have had additional sensitive information exposed, such as birthdates, addresses, and educational information if that was included in applications to academic programs.

What we are doing.

Files which include sensitive information, no longer needed for business operations, have been removed, and remaining files have been redacted or encrypted. 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 relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit my.idmonitoringservice.com to activate and take advantage of your identity monitoring services.

You have until **February 12, 2018** to activate your identity monitoring services.

Membership Number: <<Member ID>>

2520 Correa Road, ITC, 6th Floor
Honolulu, Hawai'i 96822
Telephone: (808) 956-3501
Fax: (808) 956-7322

An Equal Opportunity/Affirmative Action Institution

9301PM-1117

To receive credit services by mail instead of online, please call 1-833-210-8121. Additional information describing your services is included with this letter.

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 filing 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 identity 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 US 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:

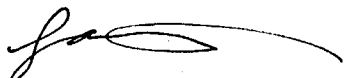
- <http://www.ed.gov/about/offices/list/oig/misused/idtheft.html>;
- <http://www.ed.gov/about/offices/list/oig/misused/victim.html>.

For more information.

If you have questions, please call 1-833-210-8121, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

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,



Garret T. Yoshimi
Vice President for IT and CIO

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.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.