UNIVERSITY OF HAWAI‘I SYSTEM ANNUAL REPORT

REPORT TO THE 2010 LEGISLATURE

Report on Security Breach
at the University of Hawai‘i West O‘ahu
October 18, 2010

HRS 487N-4

November 8, 2010

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

Discovery of Data Exposure: October 18, 2010
Location of Data Exposure: University of Hawai`i – West O`ahu (UHWO)
Nature of Data Exposure: Public Server Discovered with Sensitive Information

Incident Description:
On October 18, 2010, the University of Hawai`i was notified that sensitive information was exposed on a UHWO web server. The server was disconnected immediately from the network and an investigation launched to determine the cause of the exposure.

The situation was reported to the University by Aaron Titus, Privacy Director of the Liberty Coalition, a non-profit group based in Washington D.C. Mr. Titus discovered the files utilizing a Google site search and was able to navigate to the directories that contained the files.

Upon further investigation by the UHWO, it was learned that the files were uploaded to a UHWO faculty web server in December 2009 by a faculty member who believed the server was secured. The now retired faculty member was conducting a longitudinal study of students attending UH Mānoa between 1990-1998 and during 2001. His research may have also included students who attended UHWO during Fall 1994 or graduated from UHWO between 1988-1993.

Approximately 40,900 individuals have been identified as potentially at-risk. Notification letters have been sent to the last known postal addresses on record with the University. Additionally, a secondary email notification was sent to any email addresses on record.

A press release was issued on October 28, 2010 and a web site (http://www.uhwo.hawaii.edu/idaler) was developed to provide detailed information for any at-risk individuals. A special phone line was also established to handle any inquiries by concerned individuals.

The Honolulu Police Department and the FBI were both notified about the incident.

A copy of the notification letter is included as Attachment A.
A copy of the email notification letter is included as Attachment B.
A copy of the press release is included as Attachment C.
A copy of the UHWO web site is included as Attachment D.
A copy of the Frequently Asked Questions is included as Attachment E.
A copy of UH West Oahu's Action Plan is included as Attachment F.

UNIVERSITY of HAWAI'I® WEST O'AHU

ADDRESS
ADDRESS

Dear (FName) (LName),

We are contacting you because some of your personal information may have been inadvertently exposed, and we would like to provide guidance on how you can protect yourself from potential risks associated with this incident.

On October 18, the University of Hawai'i was notified by the Liberty Coalition, a non-profit group based in Washington, D.C., that names, Social Security numbers, birth dates and other educational information were discovered on University of Hawaii web servers. The University immediately removed access to the identified materials and is conducting an extensive investigation. Individuals potentially affected are students who attended the University of Hawai'i at Manoa between 1990-1998 and during 2001.

A University of Hawai'i – West O'ahu employee was conducting a longitudinal study of UH Manoa students. The files were obtained from the UH System's Institutional Research Office and were placed on a faculty web server that was thought to be secured. The files were placed on the server in December 2009. The Liberty Coalition discovered the files using specific Google site search strings and navigated to the directories that contained the files via the Google search results. Different files had different information on some of the individuals, but it is believed that the aggregation of the exposed files could allow matching to create the potential for identity theft.

The FBI and Honolulu Police Department have been notified. At this time, UH West O'ahu has no evidence that anyone's personal information was accessed for malicious intent. UH West O'ahu is also working with UH System to adopt more proactive security measures to ensure better privacy protection.

Affected individuals are encouraged to:

- Obtain and carefully review credit reports. Order free credits reports from all three credit agencies by going to the website at http://www.annualcreditreport.com/ or by calling 877-322-8228.
- Review bank and credit card statements regularly, and look for unusual or suspicious activities.
- Contact appropriate financial institutions immediately upon noticing any irregularity in a credit report or account.

If your accounts have been compromised, take immediate action by:

UNIVERSITY of HAWAI'I® WEST O'AHU

- Requesting a refund.
- Closing the compromised account.
- Placing a fraud alert on your credit records.
- Placing a "freeze" on your credit records.
- Filing a police report.

More information can be found on the Federal Trade Commission's website at http://www.onguardonline.gov/topics/identity-theft.aspx.

UH West O'ahu has set up an ID Alert Help-Line for you. If you have any questions, please call (808) 956-6000 on weekdays between 8:00 a.m. to 4:30 p.m. A webpage with answers to frequently asked questions is also available at www.uhwo.hawaii.edu/idalert. Updates will be posted as they become available.

Sincerely,

Ryan Mielke
Director of External Programs
and Community Outreach

Attachment B

From: Ryan Mielke - UHWO Director of External Programs - Community Outreach <announce@hawaii.edu>
Subject: **Inadvertent Exposure of Personal InformationAloha, We are contac**
Date: October 28, 2010 8:11:17 PM HST
To: announce@hawaii.edu

Aloha,

We are contacting you because some of your personal information may have been inadvertently exposed, and we would like to provide guidance on how you can protect yourself from potential risks associated with this incident.

On October 18, the University of Hawai`i was notified by the Liberty Coalition, a non-profit group based in Washington, D.C., that names, Social Security numbers, birth dates and other educational information were discovered on University of Hawaii web servers. The University immediately removed access to the identified materials and is conducting an extensive investigation. Individuals potentially affected are students who attended the University of Hawai`i at Manoa between 1990-1998 and during 2001.

We are sending this email notification to the last known email addresses that were on record with the University. You may receive multiple copies of this email if you had more than one email address recorded with the University. And it is possible that you could be receiving this notification in error. Email addresses may have been abandoned by the original owner and re-used later. If you do NOT fall in the affected group of students, please disregard this notice.

A University of Hawai`i West O`ahu employee was conducting a longitudinal study of UH Manoa students. The files were obtained from the UH System's Institutional Research Office and were placed on a faculty web server that was thought to be secured. The files were placed on the server in December 2009. The Liberty Coalition discovered the files using specific Google site search strings and navigated to the directories that contained the files via the Google search results. Different files had different information on some of the individuals, but it is believed that the aggregation of the exposed files could allow matching to create the potential for identity theft.

The FBI and Honolulu Police Department have been notified. At this time, UH West O`ahu has no evidence that anyone's personal information was accessed for malicious intent. UH West O`ahu is also working with UH System to adopt more proactive security measures to ensure better privacy protection.

Affected individuals are encouraged to:

- Obtain and carefully review credit reports. Order free credits reports from all three credit agencies by going to the website at http://www.annualcreditreport.com/ or by calling 877-322-8228.
- Review bank and credit card statements regularly, and look for unusual or suspicious activities.
- Contact appropriate financial institutions immediately upon noticing any irregularity in a credit report or account.

If your accounts have been compromised, take immediate action by:

- Requesting a refund.
- Closing the compromised account.
- Placing a fraud alert on your credit records.
- Placing a freeze on your credit records.
- Filing a police report.

More information can be found on the Federal Trade Commissions website at http://www.onguardonline.gov/topics/identity-theft.aspx.

UH West O`ahu has set up an ID Alert Help-Line for you. If you have any questions, please call (808) 956-6000 on weekdays between 8:00 a.m. to 4:30 p.m. A webpage with answers to frequently asked questions is also available at http://www.uhwo.hawaii.edu/idalert. Updates will be posted as they become available.

Sincerely,

Ryan Mielke
Director of External Programs
and Community Outreach

--

This message was sent on behalf of Ryan Mielke - UHWO Director of External Programs - Community Outreach.
Please do not reply to this message.
It was sent from an address that cannot accept incoming email.

Announcement ID number: 1288332669-680
Announcement distribution:
- A manually entered list of email addresses

Attachment C

Office of the Chancellor

UNIVERSITY of HAWAI'I® WEST O'AHU

NEWS RELEASE
Oct. XX, 2010

Media Contact: Ryan Mielke, (808) 454-4735
rmielke@uhwo.hawaii.edu

UH WEST OAHU ANNOUNCES INADVERTENT EXPOSURE OF SENSITIVE STUDENT INFORMATION

PEARL CITY – The University of Hawai`i – West O`ahu (UHWO) is notifying approximately 40,000 individuals that their personal information may have been compromised.

The exposure occurred when a faculty member inadvertently uploaded files containing data including names, social security numbers, addresses, birth dates and educational information to an unencrypted faculty web server. Individuals potentially affected are students who attended the University of Hawai`i at Manoa from 1990 – 1998 and during 2001. In addition, students who attended UHWO during Fall of 1994 or graduated from 1988 – 1993 may also be affected.

The faculty member, who is now retired from UHWO, was conducting a longitudinal study of UH Manoa students. The faculty member obtained the files from the University of Hawai`i System Institutional Research Office and placed the files containing the information onto the faculty web server in December 2009.

UHWO promptly removed the unintentionally exposed files and disconnected the affected server from the network, after Liberty Coalition, a non-profit group based in Washington D.C., notified University officials about the exposure on October 18. Different files had different information on some of the individuals, but it is believed that the aggregation of the exposed files could allow matching to create the potential for identity theft, which is highly unlikely to occur.

The FBI and Honolulu Police Department have been notified. At this time, UHWO has no evidence that anyone's personal information was accessed for malicious intent. UHWO is also working with UH System to adopt more proactive security measures to ensure better privacy protection.

Affected individuals are encouraged to:

- Obtain and carefully review credit reports. Order free credits reports from all three credit agencies by going to the website at http://www.annualcreditreport.com/ or by

calling 877-322-8228.

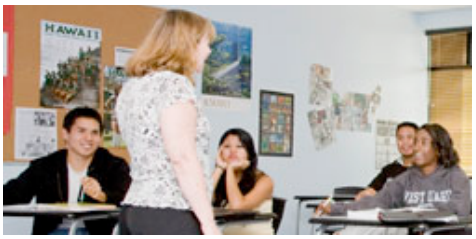
- Review bank and credit card statements regularly, and look for unusual or suspicious activities.
- Contact appropriate financial institutions immediately upon noticing any irregularity in a credit report or account.

The University is in the process of contacting the affected individuals by postal mail and email. Anyone with questions may call **(808) 956-6000 on weekdays between 8:00 a.m. – 4:30 p.m.** A webpage with answers to frequently asked questions is also available at: www.uhwo.hawaii.edu/idalert. Updates will be posted as they become available.

###

Attachment D

About UHWO




UNIVERSITY of HAWAI'I WEST O'AHU News Release

NEWS RELEASE
October 28, 2010

UH WEST O'AHU ANNOUNCES INADVERTENT EXPOSURE OF SENSITIVE STUDENT INFORMATION

PEARL CITY – The University of Hawai'i -- West O'ahu (UHWO) is notifying approximately 40,000 individuals that their personal information may have been compromised.

The exposure occurred when a faculty member inadvertently uploaded files containing data including names, social security numbers, addresses, birth dates and educational information to an unencrypted faculty web server. Individuals potentially affected are students who attended the University of Hawai'i at Mānoa from 1990 – 1998 and during 2001. In addition, students who attended UHWO during Fall of 1994 or graduated from 1988 - 1993 may also be affected.

The faculty member, who is now retired from UHWO, was conducting a longitudinal study of UH students. The faculty member obtained the files from the University of Hawai'i System Institutional Research Office and placed the files containing the information onto the faculty web server in December 2009.

UHWO promptly removed the unintentionally exposed files and disconnected the affected server from the network, after Liberty Coalition, a non-profit group based in Washington D.C., notified University officials about the exposure on October 18. Different files had different information on some of the individuals, but it is believed that the aggregation of the exposed files could allow matching to create the potential for identity theft, which is highly unlikely to occur.

The FBI and Honolulu Police Department have been notified. At this time, UHWO has no evidence that anyone's personal information was accessed for malicious intent. UHWO is also working with UH System to adopt more proactive security measures to ensure better privacy protection.

Affected individuals are encouraged to:

- Obtain and carefully review credit reports. Order free credits reports from all three credit agencies by going to the website at http://www.annualcreditreport.com/ or by calling 877-322-8228.
- Review bank and credit card statements regularly, and look for unusual or suspicious activities.
- Contact appropriate financial institutions immediately upon noticing any irregularity in a credit report or account.

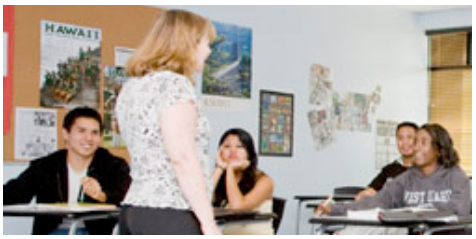
The University is in the process of contacting the affected individuals by postal mail and email. Anyone with questions may call (808) 956-6000 on weekdays between 8:00 a.m. – 4:30 p.m. A webpage with answers to frequently asked questions is also available at: www.uhwo.hawaii.edu/idalert. Updates will be posted as they become available.

Related Links

UHWO ID Alert FAQ

Attachment E

About UHWO




FREQUENTLY ASKED QUESTIONS ON INADVERTENT EXPOSURE OF SENSITIVE STUDENT INFORMATION

What happened?
On Monday, October 18, 2010 UH officials were notified of an inadvertent exposure of student information.

How did this happen?
A faculty member, who was conducting a study of UH students, uploaded files containing personal information onto an unencrypted faculty web server, which was thought to be secure.

Am I affected?
Approximately 40,000 unique SSNs were stored on the server. Student who attended UH Mānoa from 1990 – 1998 and during 2001 may be affected. In addition, students who attended UHWO during Fall of 1994 or graduated from 1988 - 1993 may also be affected.

What information was in the compromised database?
The uploaded files contained data including names, social security numbers, and may have also contained addresses, birth dates and educational information.

Has the data been misused?
At this time, University officials have no evidence that anyone's personal information was accessed for malicious intent or that any information was misused.

Was any credit card information exposed?
No. We have no evidence of any credit card or other personal financial information being exposed.

Have law enforcement authorities been notified?
The Honolulu Police Department and FBI have been notified, and have been asked to investigate any potential criminal activity related to this incident.

What is the campus doing to prevent future security breaches?
UH West Oahu is also working with UH System to adopt more proactive security measures to ensure better privacy protection. Additional security measures being taken include strengthening internal automated network monitoring practices, and performing extensive evaluations of systems to identify other potential security risks.

How will affected individuals be notified?
Letters to affected individuals were mailed on October 29, 2010, and should be received as soon as October 30, 2010. In addition, an email notice will be sent to affected individuals at their most recent email address on record.

What should affected individuals know and do?
Carefully monitor your financial information and take protective measures against identity theft, which include:

- Obtaining and carefully reviewing credit reports. Free credit reports from all three credit agencies may be obtained at http://www.annualcreditreports.com or by calling 877-322-8228.
- Reviewing bank and credit card statements regularly, and looking for unusual or suspicious activities.
- Contacting appropriate financial institutions immediately upon noticing any irregularity in a credit report or account.

If your identity or account has been compromised, you may take actions such as requesting refunds, closing accounts, and placing your credit records in a state of "fraud alert" or "freeze." Please know that we are making every effort to ensure that this incident does not recur.

If I did not receive a notification letter, does that mean my information was not in the compromised database?
Not necessarily. While every attempt has been made to identify and contact all individuals, we did not have addresses for all individuals.

How can I get more information?
On weekdays between the hours of 8:00 a.m. to 4:30 p.m., call (808) 956-6000, or go to the webpage at www.uhwo.hawaii.edu/idalert. Updates will be posted as new information becomes available.

Related Links

UHWO ID Alert Press Release

Attachment F

University of Hawai‘i – West O‘ahu
Information Security – Data Exposure
Action Plan

In addition to the notification of affected individuals, UH West O‘ahu has taken or plans the following actions:

- Ensure that all computers are updated regularly for system and application patches (such as but not limited to: operating systems, anti-virus software, web browsers, office applications)

- Strengthen internal controls governing information systems management and use by:
    - Identifying sensitive information repositories
    - Purging unneeded sensitive information
    - Securing sensitive information in accordance with UH policies
    - Communication & education on UH IT policies

- Promote information technology (IT) best practices including but not limited to:
    - Safe computing practices
    - Password management and protection
    - Safe handling & management of sensitive information and systems

- Evaluate and implement additional security measures to minimize future risks including but not limited to:
    - Network monitoring & traffic management
    - Firewalls
    - Scanning of systems for vulnerabilities