

UNIVERSITY OF HAWAI‘I SYSTEM ANNUAL REPORT



REPORT TO THE LEGISLATURE

Report on Security Breach
at the University of Hawai'i at Mānoa

HRS 487N-4

July 6, 2010

Subject: Report to the Legislature on Security Breach at the University of Hawaii at Manoa Auxiliary Enterprises Parking Office

Date of Breach: May 30, 2010
Discovery of Breach: June 15, 2010
Location of Breach: Auxiliary Enterprises – Parking Office, UH Manoa
Nature of Breach: Server with Sensitive Information Compromised

Incident Description:

On June 15, 2010, a routine audit of system logs conducted by an employee in the UH Mānoa (UHM) Auxiliary Enterprise department revealed unusual activity in the logs of a server used by the UHM Parking Office. Upon discovery of the compromise, the system was immediately isolated and an investigation launched to determine the scope of any breach. An internal investigation was initiated immediately, with support from UH Information Technology Services (ITS).

On June 24, the internal investigation concluded that unauthorized privileged access had occurred and that the server in question contained sensitive personal information. Although the investigation could neither prove nor disprove whether sensitive personal information was accessed, this information was clearly at risk of exposure.

A forensic consultant has been retained to investigate further. Reports have been filed with the FBI and HPD. Neither law enforcement agency requested delaying of notification.

The database of concern contained sensitive information on approximately 53,821 individuals. These individuals are identified as “at-risk”. Per HRS 487N, notification letters have been sent to these individuals at their last known postal mailing addresses. A secondary email notification is also being sent to the last known email address on record. A press release was issued on July 6th, 2010 and a web site (<http://www.hawaii.edu/idalert>) was set up to provide detailed information for any at-risk individuals, including those for which there is no known contact information. A special phone number and email address have been established for concerned individuals to contact UHM Auxiliary Enterprises for more information.

A copy of the notification letter is included as Attachment A.

A copy of the press release is included as Attachment B.

A copy of the Frequently Asked Questions (FAQ) about this incident is included as Attachment C.

UHM Auxiliary Enterprises has developed their Action Plan to prevent any recurrence of these types of incidents. A summary of this plan is included as Attachment D.



UNIVERSITY
of HAWAII
MĀNOA

Office of the Vice Chancellor
for Administration, Finance and Operations

July 2, 2010

FName LName
Address 1
Address 2
City, ST ZIP

Dear (FName) (LName),

We are contacting you to inform you of a recent incident that may put you at risk for identity theft and to provide guidance on how you can protect yourself from financial harm and other potential risks associated with this incident.

A routine audit conducted on June 15, 2010, discovered that unauthorized access to a computer server used by the University of Hawai'i at Mānoa (UHM) Parking Office had been initiated on May 30, 2010. A Parking Office database that was located on the server contained personal information, including names, Social Security numbers, addresses, driver's license numbers, vehicle information, and credit card information. At this time, UH Mānoa has no evidence that your personal information was actually accessed, but we also cannot determine with certainty that it was not accessed.

You are receiving this notice because you are among those whose personal information was included in the Parking Office database. The database contained data on two main groups of persons:

1. Any UHM or UH System faculty and staff member employed in 1998.
2. Anyone who had business with the UHM Parking Office between January 1, 1998 and June 30, 2009. This includes:
 - a. Anyone who purchased UHM parking permits, including staff of the University, East-West Center, UH Foundation, and Research Corporation of the UH.
 - b. Campus visitors who had a car towed or appealed a parking citation.

The database did not contain the same information about all individuals. In particular, Social Security numbers and credit card information were included for only some of the individuals in the database. Your Social Security number [was/was not] included. Your credit card information [was/was not] included.

2500 Campus Road, Hawai'i Hall 307
Honolulu, Hawai'i 96822
Telephone: (808) 956-9190
Fax: (808) 956-5136

A forensic computer expert has been retained to further investigate this matter. The Honolulu Police Department and FBI have been notified and have been asked to investigate any potential criminal activity related to this incident.

Social Security numbers are no longer used for parking transactions and are being purged from all current and historic Parking Office databases. Additional security measures that are being taken include strengthening internal automated network monitoring practices and performing extensive evaluations of our systems to identify other potential security risks.

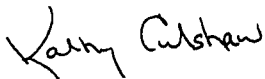
We urge you to carefully monitor your financial information and take protective measures against identity theft, which include:

- Obtaining and carefully reviewing credit reports. Free credit reports from all three credit agencies may be obtained at <http://www.annualcreditreport.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 accounts have 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 you have any questions or need additional information, you may call (808) 956-6000 on weekdays between the hours of 8:00 a.m. and 4:30 p.m, or go to webpage <http://www.hawaii.edu/idalert/> . Updates will be posted as new information becomes available.

Sincerely yours,



Kathleen Cutshaw

FOR IMMEDIATE RELEASE
July 6, 2010

Contact: Gregg Takayama, 956-9836
greggt@hawaii.edu

Diane Chang, 956-0391
dianec@hawaii.edu

UH Mānoa notifying affected individuals of online security breach of database

The University of Hawai'i at Mānoa today began notifying approximately 53,000 individuals listed in a system database, housed on a computer server used by the Parking Office, that a recent security breach may have exposed personal information—including approximately 40,870 Social Security numbers and 200 credit card numbers.

The breach occurred on May 30, 2010, and was discovered on June 15. The system was immediately isolated, and an investigation was launched to determine scope of the breach and identify individuals who may have been affected.

Letters were mailed to affected individuals on Saturday, July 3; recipients should begin receiving those letters on the next business day, Tuesday, July 6. In addition, an email notice will be sent to affected individuals at their most recent email address on record.

The FBI and Honolulu Police Department have been notified, and a forensic investigation has been initiated.

To protect personal information from further unauthorized access, Social Security numbers are no longer used for parking transactions, and are being purged from all current and historic Parking Office databases. Additional security measures that are being taken include strengthening internal automated network monitoring practices, and performing extensive evaluations of systems to identify other potential security risks.

The database contained personal information, including names, Social Security numbers, addresses, driver's license numbers, vehicle information, and credit card information of two main groups of individuals:

1. UH Mānoa faculty and staff members employed in 1998.
2. Anyone who had business with the UH Mānoa Parking Office between January 1, 1998, and June 30, 2009. This includes:
 - a. Anyone who purchased parking permits, including staff of the East-West Center, UH Foundation, and Research Corporation of the University of Hawai'i (RCUH).
 - b. Any campus visitor who had a vehicle towed or appealed a parking citation.

The possibility exists that addresses will not be located for all affected individuals—predominantly visitors to the campus who either appealed parking citations or who had vehicles towed at UH Mānoa between January 1, 1998, and June 30, 2009.

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.

Also, inquiries may be made by calling (808) 956-6000 on weekdays between the hours of 8:00 a.m. and 4:30 p.m., or by going to the webpage at <http://www.hawaii.edu/idalert/> for answers to frequently asked questions, and other related information. Updates will be posted as they become available.

Note to media: UH Mānoa spokesperson Gregg Takayama and other UH Mānoa representatives will be available for interviews at 11 a.m. today at the Hawai'i Hall lanai on the Varney Circle side of the building. Also, a copy of FAQs is attached.

###

10 Frequently Asked Questions on unauthorized access to computer server at UH Mānoa campus

1. What happened?

A routine audit conducted on June 15, 2010, discovered unauthorized access to a computer server used by the UH Mānoa Parking Office had occurred on May 30, 2010.

2. Am I affected?

Approximately 53,000 records were stored in the database. Of this total, approximately 41,000 Social Security numbers and 200 credit card numbers were exposed. The database contained data on two main groups of individuals:

1. UH Mānoa faculty and staff member employed in 1998.
2. Anyone who had business with the UH Mānoa Parking Office between January 1, 1998, and June 30, 2009. This includes:
 - a. Anyone who purchased parking permits, including staff of the East-West Center, UH Foundation and Research Corporation of the University of Hawai'i (RCUH).
 - b. Any campus visitor who had a vehicle towed or appealed a parking citation.

3. What information was in the compromised database?

The database contained personal information, including names, Social Security numbers, addresses, driver's license numbers, vehicle information, and credit card information. Information on other individuals included their UH identification numbers, which are not sensitive.

4. Has the data been misused?

At this time, UH Mānoa has no evidence that personal information was actually accessed, but we also cannot determine with certainty that it was not accessed.

5. Is there an investigation into this incident?

A forensic computer expert has been retained to further investigate this matter. The Honolulu Police Department and FBI have been notified, and have been asked to investigate any potential criminal activity related to this incident.

6. *What is the campus doing to prevent future security breaches?*

Social Security numbers are no longer used for parking transactions, and are being purged from all current and historical Parking Office databases. Additional security measures being taken include strengthening internal automated network monitoring practices, and performing extensive evaluations of systems to identify other potential security risks.

7. *How will affected individuals be notified?*

Letters to affected individuals were mailed on Saturday, July 3, 2010, and should be received starting on the next business day, Tuesday, July 6. In addition, an email notice will be sent to affected individuals at their most recent email address on record.

8. *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.

9. *If I did not receive a notification letter, does that mean my information was not in the compromised database?*

Not necessarily. The campus has been collecting addresses of affected individuals, but not all addresses could be located—predominantly visitors to the campus who either appealed parking citations or who had vehicles towed at UH Mānoa between January 1, 1998, and June 30, 2009.

10. *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 <http://www.hawaii.edu/idalert/>. Updates will be posted as new information becomes available.

###

Attachment D

University of Hawai'i at Mānoa
Auxiliary Enterprises Parking Office
Action Plan

In addition to the notification of affected individuals, Auxiliary Enterprises 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:
 - o Identifying sensitive information repositories
 - o Purging unneeded sensitive information
 - o Securing sensitive information in accordance with UH policies
 - o Communication & education on UH IT policies
- Promote information technology (IT) best practices including but not limited to:
 - o Safe computing practices
 - o Password management and protection
 - o Safe handling & management of sensitive information and systems
- Evaluate and implement additional security measures to minimize future risks including but not limited to:
 - o Network monitoring & traffic management
 - o Firewalls
 - o Scanning of systems for vulnerabilities
 - o Change management system