

SB 1162

EDT/JDL

DEPARTMENT OF HUMAN RESOURCES
CITY AND COUNTY OF HONOLULU

850 SOUTH KING STREET 10TH FLOOR • HONOLULU, HAWAII 96813
TELEPHONE: (808) 788-8500 • FAX: (808) 788-5563 • INTERNET: www.honolulu.gov/hr

PETER B. CARLISLE
MAYOR



NOEL T. ONO
DIRECTOR

January 31, 2011

The Honorable Carol Fukunaga, Chair
and Members of the Committee on Economic
Development and Technology
The Honorable Clayton Hee, Chair
and Members of the Committee on
Judiciary and Labor
The Senate
State Capitol
Honolulu, Hawaii 96813

Dear Chairs Fukunaga and Hee and Members:

Subject: Senate Bill No. 1162
Relating to Security Breaches of
Personal Information

The City & County of Honolulu, Department of Human Resources offers the following testimony with respect to Senate Bill No. 1162.

Although well-intended, the City must oppose Section 2 of the measure as it contains provisions which impose additional financial requirements on government at a time when fiscal austerity is required. At the same time, it is unclear how much training assistance the State's Information and Communication Services Division will be required to provide to the counties if the bill becomes law.

The City also opposes the portion of S.B. No. 1162 which requires that the Information Privacy and Security Council be responsible for coordinating the implementation of security breach guidelines by government agencies. To the extent such guidelines have been developed, government agencies should be allowed to maintain their autonomy to use some or all of the guidelines in responding to a security breach.

The Honorable Carol Fukunaga, Chair
and Members of the Committee on Economic
Development and Technology

The Honorable Clayton Hee, Chair
and Members of the Committee on
Judiciary and Labor

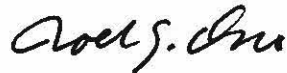
The Senate

Page 2

January 31, 2011

The City does not oppose the remaining portions of the measure. Thank you for the opportunity to testify.

Yours truly,

A handwritten signature in cursive script, appearing to read "Noel T. Ono".

Noel T. Ono
Director



Senate Committees on Economic Development and Technology
and Judiciary and Labor
Monday, January 31, 2011
1:15 p.m.

SB 1162, Relating to Security Breaches of Personal Information.

Dear Chairpersons Fukunaga and Hee and Committee Members:

On behalf of the Board of Directors of the University of Hawaii Professional Assembly (UHPA), our union supports aggressive action to address data breaches that result in the release of personal information.

Our faculty members have been subject to the University of Hawaii data breaches that resulted in the fraudulent use of personal information. The troubling aspect of the multiple unauthorized releases of data is that social security numbers may have been obtained that will not be used immediately but kept for nefarious activities in the future.

UHPA has received numerous inquiries questioning the measures taken to make all data systems more secure. For faculty members, it is not just an issue of stolen identity, it is whether research, medical, student, and academic documents are secure and protected from hackers. There are significant amounts of sensitive information throughout the UH system. The data breaches represent a growing concern as to the effectiveness of the current measures employed to provide a secured technology system.

UHPA supports the concept embodied in SB 1162, but believes that other remedies should also be implemented that includes capturing of damages of injury and out of pocket expenses. Further the appropriate security protections should be implemented and continuously upgraded as dictated by advances in technology.

Respectfully submitted,

Kristeen Hanselman
Associate Executive Director

UNIVERSITY OF HAWAII
PROFESSIONAL ASSEMBLY

1017 Palm Drive • Honolulu, Hawaii 96814-1928
Telephone: (808) 593-2157 • Facsimile: (808) 593-2160
Web Page: <http://www.uhpa.org>

GRANDE LAW OFFICES

1164 BISHOP STREET
SUITE 124-24
HONOLULU, HAWAII 96813

THOMAS R. GRANDE
tgrande@GrandeLawOffices.com

TELEPHONE: (808) 521-7500
Fax: (888) 722-5575

Senator Carol Fukunaga, Chair
Committee on Economic Development & Technology

Senator Clayton Hee, Chair
Committee on Judiciary and Labor

Hawai'i State Senate
State Capitol
415 South Beretania Street
Honolulu, Hawai'i 96813

Testimony in Support of SB 1162

Date: Monday, January 31, 2011

Time: 1:15 p.m.

Place: Conference Room 016

Chairs Fukunaga and Hee and Members of the Committees:

I am Tom Grande, co-counsel for the UH data breach victims. My co-counsel, Bruce Sherman, and I support the intent of this bill. We have several comments and suggested revisions.

Mandatory Training – SB 1162 requires mandatory training for any employee who has access to personal information. We believe that this is a good business and a good government practice that hopefully is already being put in place in light of the recent UH data breaches. However, making the training mandatory re-emphasizes its importance and ensures its completion.

Mandatory Credit Monitoring – SB 1162 provides for mandatory “credit monitoring services” to be provided for two years following the discovery of the government security breach.

We strongly agree with the intent of this provision. Businesses and government routinely offer credit monitoring services for some period of time after a data breach. We suggest however, that the option of providing a “credit report” be deleted. A credit report simply offers a snapshot of one’s credit history and does not provide the affirmative notice of problems given by credit monitoring.

GRANDE LAW OFFICES

Senator Carol Fukunaga, Chair

Senator Clayton Hee, Chair

Page 2

Public-Private Partnership

We urge the Committees to consider amending this bill to include amendments to Chapter 487N similar to those contained in SB 728, which has been referred to the Commerce & Consumer Protection and Judiciary Committees. These proposed amendments are at the end of my testimony.

The proposed amendments conform the definition of “identity theft” in Chapter 487N to that currently contained in HRS Chapter 489P. They also modify the definition of “security breach” to include conduct which exposes personal information.

Most important, the proposed amendments provide for a private statutory cause of action for data breach victims. We believe that allowing the private bar to enforce public policy statutes can be a cost-saving, public-private partnership. Cisco Systems, in its annual cybersecurity report, has looked to the European Union, where it notes that “public-private partnerships have emerged as the most promising approach to tackling many policy and operational issues around cybersecurity.” Cisco 2010 Annual Security Report at 26.

This approach is already in place in numerous consumer and business protection statutes which provide for private enforcement mechanisms to supplement government regulatory oversight.

We strongly urge the Committees to amend this bill to include a similar mechanism for data breach victims and urge the passage of this bill with our suggested amendments.

Thank you very much.

PROPOSED AMENDMENTS TO SB 1162

§487N-1 Definitions.

“Identity theft” means the unauthorized use of another person’s identifying information to obtain credit, goods, services, money, or property.

"Security breach" means an incident of unauthorized [~~access to and acquisition~~] disclosure of unencrypted or unredacted records or data containing personal information [~~where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person~~]. Any incident of unauthorized [~~access to and acquisition~~] disclosure of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach; provided that the

GRANDE LAW OFFICES

Senator Carol Fukunaga, Chair

Senator Clayton Hee, Chair

Page 3

personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

§487N-3 Penalties; civil action.

(b) In addition to any penalty provided for in subsection (a), [~~any business that violates any provision of this chapter shall be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation. The court in any action brought under this section may award reasonable attorneys' fees to the prevailing party. No such action may be brought against a government agency].~~

any person who is affected by a security breach that creates a risk of harm of identity theft may sue for damages sustained by the person. If a judgment is obtained by the plaintiff, the court shall award the plaintiff not less than \$XXX or threefold damages sustained by the plaintiff, whichever sum is greater, and reasonable attorney's fees and costs. Damages sustained by the person shall include actions taken to mitigate injury from future identity theft, including but not limited to actual or future purchase of credit report monitoring and identity theft insurance.

From: mailinglist@capitol.hawaii.gov
To: [EDTTestimony](#)
Cc: willowhi@yahoo.com
Subject: Testimony for SB1162 on 1/31/2011 1:15:00 PM
Date: Friday, January 28, 2011 7:08:48 PM

Testimony for EDT/JDL 1/31/2011 1:15:00 PM SB1162

Conference room: 016
Testifier position: oppose
Testifier will be present: No
Submitted by: Willow Aureala
Organization: Individual
Address: Ocean View, HI
Phone:
E-mail: willowhi@yahoo.com
Submitted on: 1/28/2011

Comments:

While I agree that appropriate measures need to be taken to protect mine and everyone else's privacy, requiring governmental agencies to pay for private citizen's credit reports or whatever needs to be re-considered. This really means that as a taxpayer, I'll pay for more governmental errors, and I completely disagree with this step or part of the bill. Find some other way than making me pay for yet more governmental screw-ups.

E. Dunbar
P.O.Box 861
Lihue, Hawaii 96766
Email: inunyabus@gmail.com

January 28, 2011

To: COMMITTEES - EDT/JDL, WAM
Hearing: Room 016
Date: January 31, 2011

Testimony Regarding: **SB1162**

RELATING TO SECURITY BREACHES OF PERSONAL
INFORMATION.

Information Privacy and Security Council; Appropriation

Requires government agencies to develop mandatory training programs for agency personnel to whom disclosures of personal information are made or to whom access to the personal information may be granted; in the event of a government security breach, requires the government agency to be responsible for the cost of credit report or credit monitoring services any individual affected by the breach for two years following the discovery of the security breach; requires reports of security breaches to be submitted to the information privacy and security council; requires the council to be responsible for coordination of the implementation of guidelines by government agencies; makes the comptroller or state chief information office chair of the council; authorizes the information and communication services division to provide training; appropriates funds for the council.

Aloha Chair and Members,

Act 1162 seems to create another layer of bureaucracy essentially burying deeper, any hope of clarity and adding more unnecessary spending in a critical economy and a state with no money. **Act 1162** does nothing to reprimand or punish the severe negligence that has festered so long the problem occurred four times.

The language in this bill makes me insecure. If anything it is posturing and posing to come up with a solution for something that is not fully understood. All the money that is being spent now to pass this bill and all the money that will be spent in the future when it ultimately fails and the problem recurs, is a consideration for the legislature to immediately mandate the UH to hire a top IT firm and fix the problem, at the expense

of the UH. Has anyone looked into the reason UH does not have adequate security protections in place already?

There has to be teeth in a bill for it to work:

- Tell the UH clean up their mess,
- Get rid of inefficient, incompetent or unqualified tech personnel (a good example: the big brain that took all this confidential information home with him).
- AT THE UH'S EXPENSE, they hire a top notch IT security firm (Preferably NOT from Hawaii)
- Impose PENALTIES for future breaches.

The bill's language is insufficient and dwarfs the extent of damage done to people's lives, especially the two year statute of limitations.

"487N- Personal information security; government agencies; requirements.

(b) In the event of a security breach by a government agency, the government agency shall be responsible for the costs of credit report or credit monitoring services for individuals affected by the breach for **two years** following the discovery of the security breach."

Often the damage doesn't appear for many years. The bill's language isn't taking into consideration what the UH carelessly allowed to happen and the UH DID NOT, "...acted swiftly and appropriately after discovery of the security breach, additional safeguards are necessary to ensure that the University of Hawaii and other government agencies have the resources to avoid a reoccurrence of these security breaches of personal information."

In fact it took the community a long time to get them to respond. And it has reoccurred, a total of four times.

This whole bill could be tossed and replaced with directives. It is apparent that you are seeking to legislate something that is highly technical, specialized and foreign to many.

The commitment of the legislature to act on this is appreciated but please make sure it's right.

And to think the UH wanted complete autonomy from the legislature and instead of personal information leaking this could have been germs from a Level 4 Lab.