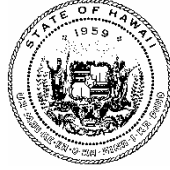


**HB 678, HD3  
Testimony**

**EDT/CPN/JDL**

NEIL ABERCROMBIE  
GOVERNOR



BRUCE A. COPPA  
Comptroller

RYAN OKAHARA  
Deputy Comptroller

STATE OF HAWAII  
DEPARTMENT OF ACCOUNTING  
AND GENERAL SERVICES  
P.O. BOX 119  
HONOLULU, HAWAII 96810-0119

TESTIMONY  
OF  
BRUCE A. COPPA, COMPTROLLER  
DEPARTMENT OF ACCOUNTING AND GENERAL SERVICES  
TO THE  
SENATE COMMITTEES  
ON  
ECONOMIC DEVELOPMENT AND TECHNOLOGY  
AND  
COMMERCE AND CONSUMER PROTECTION  
AND  
JUDICIARY AND LABOR  
ON  
March 17, 2011  
H.B. 678, H.D. 3

RELATING TO INFORMATION.

Chair Fukunaga, Chair Baker, Chair Hee, and members of the Committees, thank you for the opportunity to testify on H.B. 678, H.D. 3.

The Department of Accounting and General Services (DAGS) supports the intent of H.B. 678, H.D. 3, but has several strong concerns as follows.

1. Mandatory credit reporting requirements will increase the cost of government and business in Hawaii. Mandatory credit reporting requirements generally notify individuals after-the-fact. Although early notification can be helpful, this is less effective than stopping the crime via enhanced training before breaches occur or technical solutions that eliminate the need

for use or retention of personal information. Instead, we suggest requiring credit agencies to provide free and convenient credit freeze services to anyone who is notified of a data breach by any public or private organization. This would help prevent identity theft rather than help detect it after-the-fact. And unlike the current legislation, it would protect Hawaii residents who are notified of breaches by national organizations as well, including the federal government, credit card companies, alumni associations, hotels and online merchants. Further extension of free credit freeze services to all Hawaii residents, whether or not they have been notified of a breach, would even more strongly protect Hawaii citizens from identity theft, most of which has origins other than local data breaches. This approach would have no additional direct costs to Hawaii businesses or government and would provide significantly greater protection to consumers beyond those who might be affected by local public or private sector data breaches.

2. If required to establish and pay for credit monitoring services (or credit freeze services), for public agencies to provide commercial credit monitoring services in a timely manner, either a master contract would need to be in place or the selection of the service would need to be fully exempt from 103D. Otherwise it would be a months-long process to develop specifications and conduct a successful competitive solicitation to choose among the private for-profit vendors of these services.

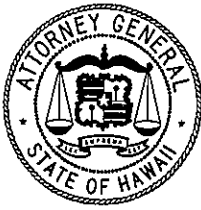
3. The requirement to have each impacted person have a choice of credit monitoring services to choose from would be logistically impractical since it would then require a public agency or business to contract with multiple credit monitoring (or credit freeze services). We would suggest the public agency or business be allowed to select one provider based on best value.

4. The requirement to have each impacted person submit their decision to not subscribe to credit monitoring (or credit freeze services) or submit their choice of credit monitoring service in writing would be logistically impractical. What would the public agency or business have to do if the impacted person failed to select an option or submit a response in writing? We would suggest the person be allowed to enroll on-line with the contracted credit monitoring service and provide an enrollment code provided to them from the public agency or business that would then grant access to that service and charge costs to the public agency or business if required (Note: If credit agencies are required to provide free credit freeze services, there would be no charges/costs to the public agency or business, simply notification that a list of individuals are eligible for their services and requesting an enrollment code).

5. Enrolling in a credit monitoring service requires provision of a full complement of personal identifying information (PII), including the SSN. This should be performed directly between the individual and the credit monitoring vendor. It would be much less secure and more time-consuming to involve the entity that performed the notification into the mechanics of providing the individual's PII to the credit monitoring vendor and executing the enrollment. This should be accomplished on-line or via phone directly by the person and the credit service provider.

DAGS recommends replacing language in H.B. 678, H.D. 3, with the language from S.B. 796, S.D. 2. And with the new language from S.B. 796, S.D. 2 inserted replace the word “business” with “government agency” and eliminating references to financial institutions.

Thank you for the opportunity to testify on this matter.



**TESTIMONY OF  
THE DEPARTMENT OF THE ATTORNEY GENERAL  
TWENTY-SIXTH LEGISLATURE, 2011**

---

**ON THE FOLLOWING MEASURE:**

H.B. NO. 678, H.D. 3, RELATING TO INFORMATION.

**BEFORE THE:**

SENATE COMMITTEES ON ECONOMIC DEVELOPMENT AND TECHNOLOGY AND ON  
COMMERCE AND CONSUMER PROTECTION AND ON JUDICIARY AND LABOR

**DATE:** Thursday, March 17, 2011      **TIME:** 9:00 a.m.

**LOCATION:** State Capitol, Room 229

**TESTIFIER(S):** David M. Louie, Attorney General, or  
Charleen M. Aina, Deputy Attorney General

---

Chairs Fukunaga, Baker, and Hee and Members of the Committees:

The Department of the Attorney General testifies to recommend that agencies be given sufficient time to implement the provisions of this bill, if the Committees intend to recommend that this measure pass Second Reading.

Under H.B. No. 678, H.D. 3, every government agency is required to give notice, and offer every person a free, three-year subscription to a nationwide consumer reporting agency's services, when the personal information the agency keeps about the person is accessed, acquired, or disclosed without authority, and is thereafter used or otherwise could be used to commit identity theft in the first, second, or third degree under the Hawaii Penal Code.

The bill's "upon its approval" effective date, anticipates that these protections against identity theft will be in place the day after the bill takes effect. This is not realistic.

The Office of Consumer Protection will need to develop and adopt appropriate rules. To devise effective procedures to implement the bill's requirements, state and county agencies will need to know how often and to what extent their information

systems could be breached, how many people could be affected by those breaches, and how much the subscriptions they must provide will cost. Revising the bill to provide an implementation deadline different from the bill's effective date will allow agencies the time needed to attend to these operational details.

Establishing that separate deadline will also give each jurisdiction (state or county) time to consider whether designating a single agency to implement the bill's requirements might be more efficient and economical. Most agency information systems are stored on centralized servers. A single security breach could result in one person receiving notice and a subscription offer from more than one agency, without the multiple agencies being aware of the competing or duplicate offers the person received.

Assigning a single agency the responsibility for issuing notices and offering subscriptions would allow jurisdictions to take advantage of economies of scale, minimize duplication, consolidate record keeping, and rely on a single, jurisdiction-wide requirements contract to purchase the nationwide consumer reporting agency services on a long-term, cost-effective basis. It would also obviate delays in issuing notices of security breaches when agencies that collect and maintain personal information, and agencies that store that information, are unable to agree which of them was the "government agency responsible for a security breach."

The Attorney General takes no position as to whether this bill should be enacted. If it is enacted, however, agencies should be given sufficient time to implement it.

We suggest revisions to make the bill clearer and more complete:

1. Replacing the paragraph at page 1 beginning at line 5 with the following:

Any government agency responsible for a security breach that provides a person with information with which to commit an offense under section 708-839.6, 708-839.7, or 708-839.8 shall notify each person whose personal information was accessed, acquired, or disclosed of the security breach, and offer the person a three-year subscription to a nationwide consumer reporting agency's services, at no cost to the person. Procurements of subscriptions to a nationwide consumer reporting agency's services for purposes of this section shall be exempt from chapter 103D.

2. Changing "of the business" to "of a business or government agency" on page 4, line 8.

3. Inserting "under section 487N-\_\_\_" after "notification" on page 5, line 5.

4. Inserting "or the recipient of a security breach notification under section 487N-\_\_\_" after "identity theft" on page 5, line 13.



NEIL AMBERCROMBIE  
GOVERNOR

BRIAN SCHATZ  
LT. GOVERNOR

STATE OF HAWAII  
OFFICE OF THE DIRECTOR  
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS  
335 MERCHANT STREET, ROOM 310  
P.O. Box 541  
HONOLULU, HAWAII 96809  
Phone Number: 586-2850  
Fax Number: 586-2856  
[www.hawaii.gov/dcca](http://www.hawaii.gov/dcca)

KEALI'I S. LOPEZ  
DIRECTOR

EVERETT KANESHIGE  
DEPUTY DIRECTOR

PRESENTATION OF THE  
OFFICE OF CONSUMER PROTECTION

TO THE SENATE COMMITTEES ON ECONOMIC DEVELOPMENT AND  
TECHNOLOGY, AND COMMERCE AND CONSUMER PROTECTION,  
AND JUDICIARY AND LABOR

TWENTY-SIXTH LEGISLATURE  
Regular Session of 2011

Thursday, March 17, 2011  
9:00 a.m.

**TESTIMONY ON HOUSE BILL NO. 678, H.D. 3, RELATING TO INFORMATION.**

TO THE HONORABLE CAROL FUKUNAGA, ROSALYN H. BAKER, AND CLAYTON  
HEE, CHAIRS, AND GLENN WAKAI, BRIAN T. TANIGUCHI AND MAILE S.L.  
SHIMABUKURO, VICE CHAIRS, AND MEMBERS OF THE COMMITTEES:

The Department of Commerce and Consumer Affairs ("Department") appreciates the opportunity to testify regarding House Bill No. 678, H.D. 3, Relating to Information. My name is Stephen Levins, and I am the Executive Director of the Office of Consumer Protection ("OCP"), representing the Department.

House Bill No. 678, H.D. 3, proposes to require government entities responsible for a security breach to pay for access to credit reports for at least three years and also expands the definition of "security breach". The Department takes no position at this



time but offers the following comments.

Under federal law, the Fair and Accurate Credit Transactions Act ("FACTA"), all Hawaii residents can receive free copies of their credit reports once a year from each of the three national credit reporting agencies -- Equifax, Experian, and Trans Union. This law provides consumers with an easier and timelier ability than ever before to determine that their credit is being fraudulently used.

To maximize the benefits of FACTA, consumer advocates advise consumers to order one report from one agency at a time, at four-month intervals. In effect, consumers now have the ability to monitor their credit reports for free three times per year. In addition to the free reports available each year, consumers are entitled to a free report from each of the agencies if they believe that they have become the victim of identity theft. To receive the free report in these circumstances, all that a victim needs to do is to contact each reporting agency directly and be prepared to provide a copy of a police report. Reviewing the credit reports enables consumers to detect fraudulent activity early and allows them to implement effective steps to limit damage resulting from potential identity theft.

The advances of FACTA notwithstanding, House Bill No. 678, H.D. 3, imposes an obligation on government entities responsible for the unauthorized release of personal information to bear the costs of providing a credit monitoring service for the potential victims. While the need for credit monitoring arises due to the action of those who release personal information, it is not clear that "credit monitoring services" are any

more valuable to consumers than the tri-annual credit reports which are now available free of charge as a consequence of FACTA.

Credit monitoring services offer their programs as "privacy protection" or "anti-ID-theft" services. They are not a deterrent to identity theft, but simply a potential early warning. The actual services provided vary widely. In general, the services promise to check a consumer's report regularly and alert them if suspicious activity is found. Many consumer groups feel that the monitoring services, which can cost up to \$200 per year, provide a service that most consumers can do for themselves for free or for considerably less than the relatively high subscription costs. If this bill becomes law, Hawaii businesses and government agencies may be placed in a position in which they will have to spend millions of dollars to comply with this measure. Consequently, imposing such a potentially significant financial burden on the affected entities may not be warranted at this time in view of the consumer-friendly changes made by FACTA.

House Bill No. 678 H.D. 3, also seeks to expand the definition of security breach to include "any incident of inadvertent, unauthorized disclosure of unencrypted or unredacted records or data containing personal information". While this amendment would appear to provide enhanced protection to affected persons of a security breach another standard worthy of consideration is the one used by the state of California, which has been adopted by the majority of states. Pursuant to this model, a security breach is defined as "an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained

Testimony on House Bill No. 678, H.D. 3  
Thursday, March 17, 2011  
Page 4

by the Entity." It is superior to current Hawaii law, since there is no requirement of "illegal conduct" and or "substantial risk to the victim". Additionally, in view of the fact that at least 27 states and the District of Columbia have in some form adopted the California definition of security breach, it is extremely unlikely that adoption of it in Hawaii will pose any significant problems to the business community.

Thank you for this opportunity to testify on House Bill No. 678, H.D. 3. I will be happy to answer any questions that the Committee members may have.

TESTIMONY OF THE AMERICAN COUNCIL OF LIFE INSURERS  
ON HB 678, HD 3, RELATING TO INFORMATION

March 17, 2011

Via e mail: [edttestimony@capitol.hawaii.gov](mailto:edttestimony@capitol.hawaii.gov)

Hon. Senator Carol Fukunaga, Chair  
Committee on Economic Development and Technology  
Hon. Senator Rosalyn H. Baker, Chair  
Committee on Commerce and Consumer Protection  
Hon. Senator Clayton Hee, Chair  
Committee on Judiciary  
State Senate  
Hawaii State Capital, Conference Room 229  
415 South Beretania Street  
Honolulu, Hawaii 96813

Dear Chair Fukunaga, Chair Baker, Chair Hee and Committee Members:

Thank you for the opportunity to testify in opposition to the proposed modifications to the definition of "Security breach" set forth in Section 2 of HB 678, HD 3, Relating to Information.

Our firm represents the American Council of Life Insurers ("ACLI"), a national trade association, which represents more than three hundred (300) legal reserve life insurer and fraternal benefit society member companies operating in the United States. ACLI member companies account for 90% of the assets and premiums of the United States life and annuity industry. Two hundred thirty-nine (239) ACLI member companies currently do business in the State of Hawaii. They represent 93% of the life insurance premiums and 95% of the annuity considerations in this State.

ACLI and its member companies recognize that their customers expect them to maintain the security of their personal information.

ACLI acknowledges that life insurers have an affirmative and continuing obligation to protect the security of their customers' personal information and strongly supports requirements for insurers to protect the security of their customers' personal information.

ACLI also supports legislation that provides standards for notification to individuals whose personal information has been subject to a security breach.

At the same time, ACLI supports legislation that avoids needlessly alarming individuals and undermining the significance of notification of a security breach - legislation that requires notification only when the security and confidentiality of personal information is truly at risk and the information is likely to be misused.

Unfortunately, however, ACLI must respectfully strongly oppose the proposed modifications to the definition of “Security breach” set forth in Section 2 of HB 678, HD 3. This definition applies to incidents involving the records or data of businesses, including insurers, as well as government agencies. The proposed modifications to the definition of “Security breach” are likely to have significant unintended harmful consequences for Hawaii consumers.

Most significantly, Section 2 of the bill would amend the definition of “security breach” to include the following:

- c) Any incident of inadvertent, unauthorized disclosure of unencrypted or unredacted records or data containing personal information . . . .

The proposed modifications will cause the definition of “security breach” to include inadvertent, unintentional disclosures of personal information - irrespective of whether affected persons are likely to be at risk of harm. They will effectively eliminate the “harm trigger” in the current definition of “security breach.”

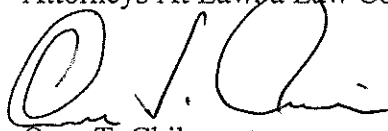
As a result of the proposed modifications to the definition of “security breach,” businesses will be required to provide affected persons with notice even when their personal information is not likely to be misused or even compromised - needlessly alarming Hawaii residents. Most importantly, the likely significant increase in the number of notices provided Hawaii residents may well undermine the importance of the notices and may cause Hawaii residents not to pay adequate attention to notices of breaches involving real threats to their personal information. In other words, the proposed modifications to the definition of “security breach” may have the unintended consequence of marginalizing the importance of real threats to consumers’ personal information.

ACLI respectfully submits that Hawaii residents will be most effectively protected if they are not overwhelmed by unnecessary notices and are provided notice only when there is a risk of harm. Accordingly, ACLI respectfully strongly urges this Committee to amend the bill by deleting the proposed modifications to the definition of “Security breach” set forth in Section 2 of the bill.

ACLI has been in discussions with other interested stakeholders in crafting language acceptable to all parties to replace the current definition in the Bill. ACLI request, therefore, that the Committees allow the parties to work out their differences prior to its decision making on the bill.

Again, thank you for the opportunity to testify in opposition to the proposed modifications to the definition of "Security breach" set forth in Section 2 of HB 698, HD 3, Relating to Information.

CHAR, HAMILTON  
CAMPBELL & YOSHIDA  
Attorneys At Law, a Law Corporation

A handwritten signature in black ink, appearing to read "Oren T. Chikamoto". The signature is stylized with a large initial "O" and a long horizontal stroke at the end.

Oren T. Chikamoto  
737 Bishop Street, Suite 2100  
Honolulu, Hawaii 96813  
Telephone: (808) 524-3800  
Facsimile: (808) 523-1714



Senator Carol Fukunaga, Chair  
Senator Glenn Wakai, Vice Chair  
Committee on Economic Development & Technology

Senator Rosalyn H. Baker, Chair  
Senator Brian T. Taniguchi, Vice Chair  
Committee on Commerce & Consumer Affairs

Senator Clayton Hee, Chair  
Senator Maile S. L. Shimabukuro, Vice Chair  
Committee on Judiciary & Labor

State Capitol, Honolulu, Hawaii 96813

HEARING      Thursday, March 17, 2011  
                    9:00 am  
                    Conference Room 229

**RE:    HB678, HD3, Relating to Information**

Chairs Fukunaga, Baker and Hee, Vice Chairs Wakai, Taniguchi and Shimabukuro, Members of the Committees:

Retail Merchants of Hawaii (RMH) is a not-for-profit trade organization representing about 200 members and over 2,000 storefronts, and is committed to supporting the retail industry and business in general in Hawaii.

**RMH opposes HB678, HD3**, which requires any government agency responsible for a security breach to pay for the costs of providing each person whose personal information was disclosed with, at a minimum, a three-year subscription to a nationwide consumer reporting agency's services. We acknowledge the Legislature's reaction to the security breach that occurred at the University of Hawaii last year, but believe that the focus of additional identity theft legislation should be on government.

**Our primary opposition to HB678, HD3, is in Section 2**, which broadens the definition of "security breach" to include any incident of inadvertent, unauthorized disclosure of unencrypted or unredacted records or data containing personal information, regardless of whether affected persons are likely to be at risk of harm. Retailers will be required to send notices even if there is no threat of compromise.

In 2007, landmark legislation was enacted to combat the growing incidents of identity theft in Hawaii. Working with DCCA, RMH developed a number of policy statements and advisories which are available to our industry.

Retailers' greatest vulnerability is in the area of payment card processing; according to the Digital Resources Group, 85% of data compromise is related to credit/debit cards and 75% to POS systems. Retailers continue to work with their financial partners to assure initial and on-going compliance with PCI standards. The process is costly, but the end result is greater security for consumers and, ultimately, retailers.

RMH respectfully requests the Chairs' consideration to allow the stakeholders additional time for further research and dialogue with the goal of crafting a measure that is workable for all and accomplishes the desired result. Thank you for the opportunity to comment on this measure.

Carol Pregill, President

# HMSA



An Independent Licensee of the Blue Cross and Blue Shield Association

March 17, 2011

The Honorable Carol Fukunaga, Chair  
Senate Committee on Economic Development and Technology  
The Honorable Rosalyn Baker, Chair  
Senate Committee on Commerce and Consumer Protection  
The Honorable Clayton Hee, Chair  
Senate Committee on Judiciary and Labor

**Re: HB 678, SD3 – Relating to Information**

Dear Chair Fukunaga, Chair Baker, Chair Hee and Members of the Committees:

The Hawaii Medical Service Association (HMSA) appreciates the opportunity to testify on HB 678 SD3 which requires any government agency responsible for a security breach to notify each individual impacted by the breach and to pay for a minimum three-year subscription to a nationwide consumer reporting agency's services for each impacted individual.

While the Bill ostensibly is directed to address a security breach in a government agency, the Bill's amended definition of a "security breach" impacts all entities, both public and private. While HMSA understands the intent of the legislation, we oppose the amended definition of a security breach.

Under current law, a security breach occurs "where illegal use of personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person." The law provides for a triggering event that results in a security breach. This Bill, however, broadens the definition to include, "(a)ny incident of inadvertent, unauthorized disclosure of unencrypted or unredacted records or data containing personal information..." Without a risk of harm provision, almost any event, including a simple, inadvertent misfiling of a document may become an alleged security breach.

The result of this would be our having to send out security breach notifications that may unnecessarily alarm our members when, in fact, no risk of harm actually exists.

HMSA is sensitive to need to be vigilant in protecting individual's personal information. We are subject to the mandates of the federal health Insurance Portability and Accountability Act of 1996 (HIPAA), which provides strict guidance on the maintenance and access to medical records and information, including notification of privacy procedures to the patient. To ensure the appropriate implementation of and compliance with HIPAA, we have a stringent training program for all of our employees.

We also are cognizant that, as we further progress in implementing electronic files, information security becomes more of a concern. That is why we have committed financial and personnel resources to constantly update our information security systems, both for our members and our employees. It would be irresponsible for us not to do so. The provision



in this Bill, while well intended, may do more harm to our efforts by requiring us to divert more of our resources to an unnecessary notification process. These are the very resources that we could be using to enhance our information security system.

Thank you for the opportunity to testify today in opposition to the Bill as it currently is worded.

Sincerely,

A handwritten signature in black ink, appearing to read 'JD', with a long horizontal stroke extending to the right.

Jennifer Diesman  
Vice President  
Government Relations

# GOODSILL ANDERSON QUINN & STIFEL

A LIMITED LIABILITY LAW PARTNERSHIP LLP

GOVERNMENT RELATIONS TEAM:  
GARY M. SLOVIN  
ANNE T. HORIUCHI  
MIHOKO E. ITO  
CHRISTINA ZAHARA NOH  
CHRISTINE OGAWA KARAMATSU

ALII PLACE, SUITE 1800 • 1099 ALAKEA STREET  
HONOLULU, HAWAII 96813

MAIL ADDRESS: P.O. BOX 3196  
HONOLULU, HAWAII 96801

TELEPHONE (808) 547-5600 • FAX (808) 547-5880  
info@goodsill.com • www.goodsill.com

INTERNET:  
gslovin@goodsill.com  
ahoriuchi@goodsill.com  
meito@goodsill.com  
cnoh@goodsill.com  
ckaramatsu@goodsill.com

**TO:** Senator Carol Fukunaga  
Chair, Committee on Economic Development and Technology  
Senator Rosalyn H. Baker  
Chair, Committee on Commerce and Consumer Protection  
Senator Clayton Hee  
Chair, Committee on Judiciary and Labor  
*Via Email: [EDTTestimony@Capitol.hawaii.gov](mailto:EDTTestimony@Capitol.hawaii.gov)*

**FROM:** Gary M. Slovin / Mihoko E. Ito

**DATE:** March 16, 2011

**RE:** **H.B. 678, H.D. 3 – Relating to Information**  
**Hearing: Thursday, March 17, 2011 at 9:00 a.m., Room 229**

---

Dear Chairs Fukunaga, Baker and Hee and Members of the Committees:

We respectfully submit this testimony on behalf of the Consumer Data Industry Association (CDIA). Founded in 1906, CDIA is the international trade association that represents more than 400 data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, fraud prevention, risk management, employment reporting, tenant screening and collection services.

Overall, CDIA **opposes** H.B. 678, HD 3.

## **Free Security Freeze for Security Breach**

CDIA strongly opposes Section 3 of H.B. 678 HD 3 at page 4, which amends HRS Section 489P-3 and would require nationwide consumer reporting agencies to give away free security freezes for consumers who receive security breach notices from public and private entities. Consumer reporting agencies already provide credit freeze services for Hawaii consumers and they provide those services for free to identity theft victims. Even before laws required free freezes for ID theft victims, consumer reporting agencies provided free freezes to these consumers.

March 16, 2011

Page 2

Consumer reporting agencies should not be required to give its credit freeze services away for free for non-identity theft victims (i.e., those who merely receive breach notices). Under Hawaii law, consumer reporting agencies cannot charge more than \$5.00 to place a freeze on a credit file for non-victims. This amount is less than the standard fee that these agencies are allowed to recover in many other states.

It is neither fair nor appropriate to force consumer reporting agencies to give away its freeze service for free to non-identity theft victims. Consumer reporting agencies, who are not the cause of security breaches, should not be forced to bear the costs of other business or government data breaches. Accordingly, CDIA would ask that this section be removed from the bill.

### **Definition of “Security Breach”**

CDIA also opposes changing the definition of “security breach” in Section 2 of H.B. 678 HD 3. This section substantially expands the existing definition of security breach from access of personal information that harms or is likely to cause a risk of harm to simply state that any disclosure of information in a way that will create significant additional burdens on businesses. Existing protections and penalties under federal and state law already exist, and expanding the law at this time and imposing significant burdens on the private sector is simply unjustified.

### **Government payment for credit monitoring reports**

Finally, with respect to Section 1 of H.B. 678 HD 3, CDIA generally supports the intent of requiring government agencies to be responsible for its security breaches. In addition, we support the amendments made to clarify the definition of nationwide consumer reporting agencies to be consistent with federal law. However, CDIA questions whether the monitoring program would be feasible overall.

CDIA notes that it is actively working with other stakeholders to develop language that would focus the bill on preventing data security breaches and minimizing the chances of personal information being used inappropriately after a security breach, while being mindful of the impact on those parties that are not responsible for the breach.

Thank you very much for the opportunity to testify.

**From:** [mailinglist@capitol.hawaii.gov](mailto:mailinglist@capitol.hawaii.gov)  
**To:** [EDTTestimony](#)  
**Cc:** [swartzg001@hawaii.rr.com](mailto:swartzg001@hawaii.rr.com)  
**Subject:** Testimony for HB678 on 3/17/2011 9:00:00 AM  
**Date:** Tuesday, March 15, 2011 11:13:35 PM

---

Testimony for EDT/CPN/JDL 3/17/2011 9:00:00 AM HB678

Conference room: 229  
Testifier position: oppose  
Testifier will be present: No  
Submitted by: gregory swartz  
Organization: Individual  
Address:  
Phone:  
E-mail: [swartzg001@hawaii.rr.com](mailto:swartzg001@hawaii.rr.com)  
Submitted on: 3/15/2011

Comments:

Although I am a victim of improper release of my personal information by a governmental agency. I think this bill is a waste of money. Besides, the costs of remedying the impact of improper disclosures can potentially go well beyond credit monitoring.



46-063 Emepela Pl. #U101 Kaneohe, HI 96744 · (808) 679-7454 · Kris Coffield · Co-founder/Legislative Director

---

## TESTIMONY ON HOUSE BILL 678, HOUSE DRAFT 3, RELATING TO INFORMATION

Senate Committee on Economic Development and Technology  
Hon. Carol Fukunaga, Chair  
Hon. Glenn Wakai, Vice Chair

Thursday, March 17, 2011, 9:00 AM  
State Capitol, Conference Room 229

Honorable Chair Fukunaga and committee members:

I am Kris Coffield, representing the Imua Alliance, a nonpartisan political advocacy organization that currently boasts over 60 local members. On behalf of our members, we offer this testimony in strong support of HB 678, HD3, relating to information, with consideration for a minor amendment.

As you are undoubtedly aware, a security breach at the University of Hawaii, in October of 2010, exposed the personal information of approximately 40,000 students and faculty to the public, allegedly when a faculty member mistook a public server for a private server. Information bared by the breach included names, addresses and Social Security numbers. This follows a similar breach at the college, in July of 2010, in which the credit card information, driver's license numbers and vehicle information of up to 53,000 people was jeopardized, and a further breach, in May of 2009, that placed at risk the information of 15,000 financial aid applicants at Kapi'olani Community College because of a malware infection. All told, over 250,000 private records held by the university have been inadvertently compromised in the past seven years, earning the university the grade of "F" for online security from The Liberty Coalition.

While such lapses are appalling, their potential origins are by no means limited to public institutions and agencies. Every day, residents of the state engage in transactions with local businesses and government agencies—from banks and insurance providers to employment assistance centers and the Department of Health—that require the authorized use of private information. Students of the university and private citizens, like me, have little recourse when data breaches occur, aside from costly and prolonged litigation (lawsuits resulting from the two most recent UH breaches, for example, could cost the university nearly \$10 million each, if the Ponemon Institute's \$204 average per-person legal compensation figure is to be believed). Requiring offending institutions and businesses to provide subscriptions to credit reporting agencies for at least three years provides another alternative, one that may make victims less inclined to seek court ordered remuneration.

That said, I would encourage the committee to insert language into the proposed bill mandating the written provision of potential credit reporting subscriptions not more than seven days after a breach has transpired, thus amending the first sentence of §487N- (b) to read: “No later than seven calendar days after a business or government agency provides notice of the security breach, the business or government agency responsible for the security breach shall provide each person, in writing, with a choice of not less than two credit reporting agencies from which the person may select to subscribe.” While mass security breaches, like those occurring at UH, practically necessitate written correspondence due to the sheer volume of impacted individuals, smaller breaches, should they emerge, may not. Nonetheless, persons affected by such breaches should be entitled to a written record of not only the breach, but all actions taken to resolve the problem, once discovered. Moreover, it may be advisable to add language to the measure mandating that the offending business or government agency notify victims of enrollment, once a victim has selected a credit reporting agency and been provided with a subscription. Since this legislation directs businesses and government agencies to manage enrollment on behalf of individuals, all efforts should be taken to maximize communication between persons responsible for the alleviation of a breach and persons whose privacy has been impugned.

Mahalo for the opportunity to testify in support of this bill.

Sincerely,  
Kris Coffield  
*Legislative Director*  
IMUAlliance

DEPARTMENT OF HUMAN RESOURCES

**CITY AND COUNTY OF HONOLULU**

650 SOUTH KING STREET 10<sup>TH</sup> FLOOR • HONOLULU, HAWAII 96813  
TELEPHONE: (808) 768-8500 • FAX: (808) 768-5563 • INTERNET: [www.honolulu.gov/hr](http://www.honolulu.gov/hr)

PETER B. CARLISLE  
MAYOR



NOEL T. ONO  
DIRECTOR

March 17, 2011

The Honorable Carol Fukunaga, Chair  
and Members of the Committee on Economic  
Development and Technology  
The Honorable Rosalyn H. Baker, Chair  
and Members of the Committee on Commerce  
and Consumer Protection  
The Honorable Clayton Hee, Chair  
and Members of the Committee on Judiciary and Labor  
The Senate  
State Capitol  
Honolulu, Hawaii 96813

Dear Chairs Fukunaga, Baker and Hee and Members:

Subject: House Bill No. 678, HD3, Relating to Information

The City & County of Honolulu, Department of Human Resources, respectfully opposes House Bill No. 678, HD3.

Although well-intended, the City must oppose the measure as the requirement to pay for credit monitoring imposes a significant financial requirement on government at a time when fiscal austerity is required. The amount that it would cost the City to provide a three-year subscription to a credit monitoring service as required by Section 1 of House Bill No. 678, HD3, would be overwhelming. At the same time, the service which is mandated under the bill fails to offer the level of protection that security credit freeze services are able to provide. Insofar as Section 3 of the bill already proposes to allow a consumer to place a security credit freeze on his or her credit report following receipt of a security breach notification, we urge the Committee to delete Section 1 of the House Bill No. 678, HD3.

The Honorable Carol Fukunaga, Chair  
and Members of the Committee on Economic  
Development and Technology  
The Honorable Rosalyn H. Baker, Chair  
and Members of the Committee on Commerce  
and Consumer Protection  
The Honorable Clayton Hee, Chair  
and Members of the Committee on Judiciary and Labor  
The Senate

The City further suggests that the definition of "Security breach" set forth in Section 2 of the current measure be amended to read as follows:

Does not include good faith acquisition or disclosure of personal information by an employee or agent of the business or government agency for a legitimate purpose; provided that the personal information is not used for a purpose other than a lawful purpose of the business or government agency and is not subject to further unauthorized disclosure.

The foregoing amendment provides uniformity should the revisions which the bill proposes to subsection (1)(C) of the definition be passed into law. In addition, the addition of "government agency" to the paragraph will make the definition of "Security breach" consistent with the rest of HRS Chapter 487N, since government agencies are also subject to the disclosure notification requirements set forth therein.

Thank you for this opportunity to testify.

Yours truly,

  
 Noel T. Ono  
Director



# State Privacy and Security Coalition, Inc.

TESTIMONY ON HB 678 HD3  
RELATING TO INFORMATION  
BY

JEANNINE SOUKI  
ON BEHALF OF THE  
STATE PRIVACY AND SECURITY COALITION

LATE TESTIMONY

March 17, 2011

The Honorable Carol Fukunaga, Chair  
Economic Development and Technology Committee

The Honorable Rosalyn H. Baker, Chair  
Commerce and Consumer Protection Committee

The Honorable Clayton Hee, Chair  
Judiciary and Labor

Re: Opposition to HB 678 HD3 - RELATING TO INFORMATION  
March 17, 2011, 9:00 am, Conference Room 229, Hawaii State Capitol

Dear Chairs Fukunaga, Baker, and Hee, Vice Chairs and Members of the Committees:

As a coalition of leading technology companies and technology trade associations, we write in opposition to HB 678 HD3 and the current version of SB796 SD2.

After the data security breach that occurred at the University of Hawaii last year, it is understandable that the legislature is looking for solutions. However, Hawaii already has a strong security breach law that is in many ways broader and stronger than laws in the vast majority of states. While well-intentioned, these bills would single out Hawaii businesses – who had nothing to do with University data breaches – for the risk of costly class action lawsuits absent any harm to state residents and risks harming the State’s economy at a sensitive time.

S.B.796, S.D. 2 and H.B. 678, H.D. 3, would significantly expand the definition of “security breach” under Hawaii law by adding language to the definition of security breach to include “any incident of inadvertent, unauthorized disclosure of unencrypted or unredacted records or data containing personal information.” Under the current definition, a security breach is “triggered,” and notice of the breach is required to be provided affected residents “where illegal use of personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person.”

The proposed modifications to the definition of “security breach” would effectively eliminate the existing “harm trigger” in the definition. They would cause the definition to include

500 8th Street, NW  
Washington, DC 20004  
202.799.4000 Tel  
202.799.5000 Fax

inadvertent, unintentional disclosures of personal information – irrespective of whether affected persons are likely to be at risk of harm.

They would cause the mere loss of paper documents, without any appreciable risk of harm, to trigger a breach notice obligation – a requirement found almost nowhere in the U.S.

They would require companies to send breach notifications likely to unnecessarily alarm consumers, where no risk of harm actually exists. They are likely to marginalize the importance of real threats to the security of consumers' personal information.

They are likely to result in burdensome, costly notice expenses for companies doing business in Hawaii - particularly for local Hawaii businesses that have paper records containing personal information – on retailer credit card slips, credit and mortgage applications, real estate contracts, and other paper documents that consumers fill out.

Although businesses had no involvement in the University of Hawaii security breach, the proposed modifications to the definition of “security breach” in S.B.796, S.D. 2 and H.B. 678, H.D. 3, are likely to be costly and burdensome for local businesses and other companies that do business in Hawaii - as well as to have significant unintended harmful consequences for Hawaii consumers. This bill would fall particularly heavily on Hawaii businesses. Hawaii is one of just five states to treat breaches of paper documents as security breaches. It is precisely local businesses that have paper records containing personal information – in retailer credit card slips, credit, mortgage and insurance applications, real estate contracts, the other documents that consumers fill out.

However, if it is the Committees' intent to move forward a version of this bill, we respectfully ask that you allow stakeholders additional time to work on language addressing these concerns, which if unchanged will result in very serious liability and would fall particularly heavily on Hawaii businesses.

Sincerely,

AT&T  
Internet Alliance  
NetChoice  
Oceanic Time Warner Cable  
Reed Elsevier/LexisNexis  
TechAmerica  
Verizon