

**LATE**  
**SB728**

Presentation to the Senate Committee on Commerce and Consumer Protection  
Presentation to the Senate Committee on Economic Development and Technology

Tuesday, February 8, 2011, at 8:30 a.m.

Testimony on Senate Bill 728 Relating to Information Privacy

TO: The Honorable Rosalyn H. Baker, Chair  
The Honorable Brian T. Taniguchi, Vice Chair  
Members of the Senate Committee on Commerce and Consumer Protection

TO: The Honorable Carol Fukunaga, Chair  
The Honorable Glenn Wakai, Vice Chair  
Members of the Senate Committee on Economic Development and Technology

My name is Neal Okabayashi and I testify for the Hawaii Bankers Association. While we acknowledge and are sympathetic to concerns on identity theft, we respectfully ask that this committee hold this bill because it does not adequately balance the needs of those damaged by identity theft and businesses that may have to pay more than actual damages.

It is ironic that while it has been governmental entities that have been most prominent in security breach incidents, they would continue to be exempt from paying damage claims.

HBA is most concerned about provisions reducing the standard for filing a lawsuit. Presently, anyone damaged by identity theft may file a lawsuit to recover damages. Under this bill, a person who may suffer harm can sue for damages (instead of the traditional standard of someone who did suffer harm) without any requirement to prove damages because statutory damages are awarded.

The provision for treble damages for what is not an unfair or deceptive trade act or practice nor an intentional act is inappropriate in the circumstances.

The bill should also require that a person use the federal and state remedies. For example, under Section 489P-3, a person can freeze his or her credit report which means credit monitoring service or identity theft insurance is not necessary. Under the Fair and Accurate Credit Transactions Act of 2003, a person can obtain free credit reports and initiating a fraud alert or active duty alert.

I would be happy to answer any questions you may have.



1654 South King Street  
Honolulu, Hawaii 96826-2097  
Telephone: (808) 941.0556  
Fax: (808) 945.0019  
Web site: [www.hcul.org](http://www.hcul.org)  
Email: [info@hcul.org](mailto:info@hcul.org)



11/12

Testimony to the Senate Committee on Commerce and Consumer Protection and  
Committee on Economic Development and Technology

Testimony in opposition to SB 728, Relating to Information Privacy

To: The Honorable Rosalyn Baker, Chair  
The Honorable Brian Taniguchi, Vice-Chair  
Members of the Committee on Commerce and Consumer Protection

The Honorable Carol Fukunaga, Chair  
The Honorable Glenn Wakai, Vice-Chair  
Members of the Committee on Economic Development and Technology

My name is Stefanie Sakamoto and I am testifying on behalf of the Hawaii Credit Union League, the local trade association for 85 Hawaii credit unions, representing approximately 810,000 credit union members across the state.

We are in opposition to SB 728, Relating to Information Privacy. While we understand and are sympathetic to the concerns of this bill, we are in opposition because laws already exist for those who fall victim to a data breach. Credit unions in Hawaii are in full compliance with the state and federal laws that are already in place.

Thank you for the opportunity to testify.



LATE

Senate Committees on Commerce and Consumer Protection  
and Economic Development and Technology  
Tuesday, February 8, 2011  
8:30 a.m.

**SB 728, Relating to Information Privacy.**

Dear Chairpersons Baker and Fukunaga 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 harm from identity theft.

Many faculty members and students have been victimized by data breaches at the University of Hawaii over the last five years. These breaches mean that the unauthorized use of social security numbers that may have been obtained may not be used immediately but kept for nefarious activities in the future.

The lack of appropriate notice and remedies within the state is of concern. It is important that legislation be passed that requires notice of incidents, as well as allowing recapturing of damages that may result. Defining identity theft is an important element of new legislation.

However, SB 728, while allowing an individual to sue for damages with a private entity, does not allow a similar action against a government agency. UHPA believes that a government agency also has obligations to mitigate harm. This legislation does not go far enough to protect individuals who have given confidential information to a public agency only to find that there is no cause of action when a data breach occurs.

UHPA hopes the committee will consider amendments that make it possible for victims of identity theft to seek relief from a government agency.

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>



TESTIMONY OF THE AMERICAN COUNCIL OF LIFE INSURERS  
IN OPPOSITION TO SENATE BILL 728, RELATING TO INFORMATION PRIVACY

February 8, 2011

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

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

LAIE

Dear Chair Baker, Chair Fukunaga and Committee Members:

Thank you for the opportunity to testify in opposition to Senate Bill 728, relating to Information Privacy.

Our firm represents the American Council of Life Insurers ("ACLI"), a national trade association, who represents more than three hundred (300) legal reserve life insurer and fraternal benefit society member companies operating in the United States. These member companies account for 90% of the assets and premiums of the United States Life and annuity industry. ACLI member company assets account for 91% of legal reserve company total assets. Two hundred thirty-nine (239) ACLI member companies currently do business in the State of Hawaii; and 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.

Accordingly, ACLI must respectfully strongly oppose SB 728.

SB 728 will not enhance protection of the security of Hawaii consumers' personal information and is likely to have significant unintended harmful consequences.

SB 728 will not increase security protection because it only provides for "after the fact" remedies, such as a private right of action and increased penalties and damages for breaches that already have occurred.

SB 728 does not provide for any measures to prevent future security breaches – such as requirements for government agencies and businesses to have reasonable security programs and to train staff to implement such programs.

SB 728 could have significant harmful consequences for Hawaii consumers:

The amendments to the definition of "security breach," to eliminate the requirement of a "risk of harm," and to extend even to inadvertent unauthorized disclosures, are likely to result in the provision of notices of "security breaches" that will needlessly alarm Hawaii residents when their personal information is unlikely to be misused and to marginalize the importance of real threats to consumers' personal information.

The requirement that notices include information regarding types of fraudulent activities that could result also is likely to give rise to unnecessary concern and possible alarm.

The provisions for an enhanced private right of action and to increase the penalties for breaches are unnecessary given current provisions for actual damages in the Hawaii breach law.

Most importantly, these provisions are unlikely to increase the security of Hawaii residents' personal information.

They would appear to be unnecessarily punitive – particularly in light of the proposed broadening of the definition of "security breach" and likely to give rise to unnecessary increased litigation.

The provision for damages to include payment for actions to mitigate injury from future identity theft, including actual or future purchase of credit report monitoring and identity theft insurance, is not only open-ended, but unlikely to necessarily provide increased security protection for Hawaii residents' personal information - since the benefits that may be derived from credit monitoring are questionable and very dependent on the nature of the service and the particular company.

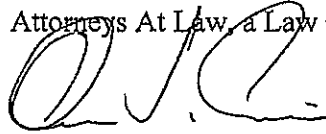
The provision for the bill to apply retroactively to July 1, 2009, would not only appear unwarranted, but is very likely to be unworkable and unenforceable.

In sum, to prevent future security breaches and avoid likely unintentional adverse consequences of the current language of SB 728, ACLI respectfully strongly urges substitution of the current language of the bill with language that would require any business or government agency that conducts business in Hawaii and owns or licenses personal information of residents of Hawaii to: (i) implement and maintain reasonable security procedures and practices; and (ii) train their employees or staff, as appropriate, to implement the procedures and practices.

Attached is a draft of an SD 1 which ACLI respectfully urges this Committee to consider. The draft SD 1 replaces its provisions with those currently in the bill. ACLI requests that this Committee defer decision making on the bill to allow other stakeholders an opportunity to review the proposed SD 1.

Again, thank you for the opportunity to testify in opposition to SB 728, relating to Information Privacy.

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



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

---

---

## A BILL FOR AN ACT

RELATING TO INFORMATION PRIVACY.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

1           SECTION 1. Chapter 487N, Hawaii Revised Statutes, is  
2 amended by adding a new section to be appropriately designated  
3 and to read as follows:

4           "§487N- Security program. (a) A business or government  
5 agency that owns or licenses personal information about a Hawaii  
6 resident shall implement and maintain reasonable security  
7 procedures and practices appropriate to the nature of the  
8 information, and to the size and complexity of the business or  
9 government agency and the nature and scope of its activities.  
10 The procedures and practices shall be designed to protect the  
11 personal information from unauthorized access, destruction, use,  
12 modification, or disclosure.

13           (b) A business or government agency shall train its staff,  
14 as appropriate, to implement the business or government agency's  
15 security program.

16           (c) A business or government agency that discloses personal  
17 information about a Hawaii resident pursuant to a contract with a



1 nonaffiliated third party shall require by contract that the  
2 third party implement and maintain reasonable security procedures  
3 and practices appropriate to the nature of the information, to  
4 protect the personal information from unauthorized access,  
5 destruction, use, modification, or disclosure."

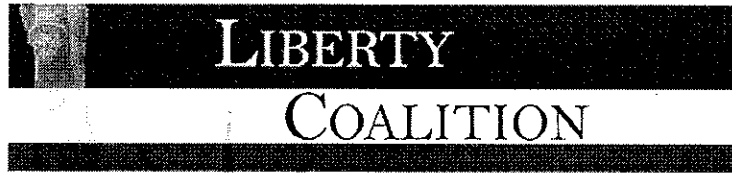
6 SECTION 2. New statutory material is underscored.

7 SECTION 3. This Act shall take effect upon its approval.

# Testimony Regarding Hawai'i SB 728

---

1/11



722 12th Street, NW  
Suite 400  
Washington DC 20005

*February 7, 2011*

*Aaron Titus, Information Privacy Director  
Liberty Coalition*

Chairpersons Baker and Fukunaga, Vice Chairpersons Taniguchi and Wakai, and Members of the Hawaii Senate Committee on Commerce and Consumer Protection and Committee on Economic Development and Technology, thank you for allowing me to testify.

My name is Aaron Titus. I am the Privacy Director for the Liberty Coalition and an attorney. The Liberty Coalition works with more than 80 partner organizations from across the political spectrum<sup>1</sup> to preserve the Bill of Rights, personal autonomy and individual privacy.

---

<sup>1</sup> The Liberty Coalition does not speak for its Coalition Partners. Liberty Coalition Partners currently include: Alliance for Patient Safety, American Association for Health Freedom, American Association of Small Property Owners, American Civil Liberties Union, American Families United, American Policy Center, Americans for Tax Reform, Amnesty International, Andrew Jackson Society, Appeal for Privacy Foundation, Arab American Institute, Association of American Physicians and Surgeons, Bill of Rights Defense Committee, Bob Barr, former Member of Congress, and Chairman and CEO of Liberty Strategies, LLC, Boston Tea Party, Campaign For Liberty, Center for Financial Privacy and Human Rights, Chicago Committee to Defend the Bill of Rights, Citizens Against Government Waste, Citizens for Health, Citizens in Charge Foundation, Clinical Social Work Federation, Common Cause, Competitive Enterprise Institute, Concerned Foreign Service Officers, (CARCLE) Congress Against Racism and Corruption in Law Enforcement, Cyber Privacy Project, Criminal Justice Policy Foundation, Citizen Outreach, Citizens Committee for the Right to Keep and Bear Arms, Center for Liberty & Community, Defending Dissent Foundation, Democrats.com, DownsizeDC.org, Drug Policy Alliance, Educator Roundtable, Ethics in Government Group, Electronic Frontier Foundation, Electronic Privacy Information Center, Equal Justice Alliance, Fairfax County Privacy Council, First Amendment Foundation, The Freedom and Justice Foundation, Government Accountability Project, International Center for the Study of Psychiatry and Psychology (ICSPP), Institute for Liberty, International Association of Whistleblowers, The Libertarian Party, Libertarian Party of Texas, Liberty Dollar, Meyda Online Info Security, Privacy, and Liberties Studies, Mothers Against the Draft, MoveOn.org Political Action, The Multiracial

The Liberty Coalition does not speak on behalf of these organizations, and this report may not reflect the position of any single Coalition Partner.

Following a large breach by the University of Hawaii in October, 2010, the Liberty Coalition issued a survey of Hawaii breaches on November 17, 2010. The report found that:

- Since 2005, at least 479,000 Hawaii records have been breached: One for every three residents.
- The University of Hawaii is responsible for 54% of all breaches in Hawaii (259,000 records), more than all other Hawaii organizations combined.
- The University of Hawaii has a pattern of breaches and unfulfilled promises.
- Organizations do not have adequate market incentives to keep personal information secure.
- Victims cannot know which breach caused identity fraud, cannot hold organizations accountable, or protect themselves.
- After a brief rest from breaches in 2008, Hawaii is experiencing another spike in reported breaches.

On December 20, 2010 the Liberty Coalition issued another 22-page report outlining legislative solutions which would decrease breaches of personal information, specifically tailored for the State of Hawaii.

These suggestions included:

- Victims of personal information breaches are 4 times more likely to be victims of identity theft, and 20% of breach victims suffer ID Theft.
- In Hawaii, more than 95,000 breach victims will likely suffer ID Theft, costing businesses and banks an estimated \$571 million and costing consumers more than \$40 million out-of-pocket.
- Establish an Identity Fraud Watchdog Agency or non-profit organization;
- Create a Victims' Trust Account to cover costs of breaches;
- Close the "Deception Loophole" and make Hawaii's State agencies accountable for deceptive trade practices, if they perform services like private companies;
- Create a private right of action for breach victims, and give victims enough information to analyze their own risk.

---

Activist, Muslim Public Affairs Council, National Coalition of Mental Health Professionals and Consumer, National Coalition of Organized Women (NCOW), National Iranian American Council, National Judicial Conduct and Disability Law Project, Inc., National Security Whistleblowers Coalition, National Whistleblowers Center, Natural Solutions Foundation, New Grady Coalition, New York Tax Reform Organization, OpenCarry.org, Pain Relief Network, People for the American Way, Patient Privacy Rights Foundation, Privacy Activism, Pullins Report, Reason Foundation, Republican Liberty Caucus, Rutherford Institute, Semmelweis Society International, Inc., The 3.5.7 Commission, Townhall, U.S. Bill of Rights Foundation, VelvetRevolution.us, Veterans Affairs Whistleblowers Coalition, Virginia Citizens Defense League, Inc., and The Woodhull Freedom Foundation.

## **Hawaii's Statutes Lack Consumer Protections for Breach Victims**

Since 2006, 45 states including Hawaii, have enacted legislation to provide statutory requirements for: 1) specific protections to prevent disclosure of Social Security Numbers and affirmative obligations to safeguard person information; 2) the proper destruction of records containing personal information that are no longer need; and 3) notification of unauthorized breaches of personal information.<sup>2</sup>

This statutory framework lacks a fourth important element—consumer protections in the event of a data breach. These consumer protections are needed to prevent and remediate identity fraud which may occur as a result of data breaches.

## **Lack of Information Leaves Victims Powerless**

Even though Hawaii requires organizations to notify victims when breaches occur, the notifications fail to give victims sufficient information to understand their level of risk, and the actions they should take. Even well-intentioned organizations issue vague, incomplete, blame-shifting or liability-reducing press releases that leave victims in the dark. And your credit report will never tell you where a thief got your social security number.

As a result, breach notification laws are not working. According to James Van Dyke, a leading identify theft expert, "notification is not working. Consumers apparently do not understand that the data breach puts them at increased risk for other types of fraud. Notification may need to be more explicit about the possible types of fraud that may be perpetrated with the data exposed, and the possible steps the consumer can take for protection."<sup>3</sup>

## **Hawaii's Breach Notification Law is Ineffective**

Notwithstanding Hawaii's breach notification law, the state seems to be experiencing an upswing in reported breaches. Breaches in Hawaii appear to be consistent with Verizon's annual data breach report in conjunction with the U.S. Secret Service,<sup>4</sup> issued in July, 2010. The report finds that most breaches "continue to be discovered by external parties and then only after a considerable amount of time," and that most organizations "remain sluggish in detecting and responding to incidents."

---

<sup>2</sup> Lazzarotti, *State Data Privacy and Security Laws, 2008 Emerging Issues*, 1879 n. 23 (Matthew Bender 2008).

<sup>3</sup> Javelin Strategy & Research, *Data Breach Notifications: Victims Face Four Times Higher Risk of Fraud* (October 2009) at 16 available at <http://www.javelinstrategy.com/reports/143/221/data-breach-notifications-victims-face-four-times-higher-risk-of-fraud> (Accessed December 15, 2010).

<sup>4</sup> *2010 Data Breach Report From Verizon Business, U.S. Secret Service Offers New Cybercrime Insights*, <http://newscenter.verizon.com/press-releases/verizon/2010/2010-data-breach-report-from.html> (Accessed December 10, 2010).

The business environment is optimized to maximize profits, and too often IT security is treated as an expense rather than an investment. Regulated industries and to a lesser extent market-driven industries are more likely to make security a priority. But since Public Relations damage is the largest (and often the only) liability following a breach, many organizations spend most of their resources on PR damage control rather than substantive improvements to security.

## **SB 728 is Good for Hawaii Residents**

SB 728 will give consumers a much-needed private right of action to recover for the damages associated with credit monitoring services, time off work to deal with creditors, and living with a proverbial Sword of Damocles over their heads.

Just as importantly, SB 728 will amend Hawaii's Breach Notification Law to require breaching organizations to include enough information about a breach to empower victims to come to an educated conclusion to the level of risk they face. At a minimum, each breach notification must include the following information:

- **Distribution Method.** An online breach carries substantially more risk than the temporary release of paper documents in a dumpster, because an online breach is available to many more people. Victims must know the distribution medium and method in order to understand their risk.
- **Duration of Exposure.** The risk of unauthorized access is more for information exposed for a long period of time (e.g. 1 year) versus a short period of time (e.g. 1 hour)
- **Types of Information Exposed.** Knowing the type of information exposed is vital before a person can assess the risk he or she faces. Social Security numbers are sensitive for almost everybody, but exposing an address online might be a matter of life and death for a victim of domestic violence.
- **Possible Types of Fraud.** The report should name possible types of fraud that may be perpetrated with the exposed data, and possible remedial steps the individual can take.
- **Statement of Legal Rights and Responsibilities.** The letter should state all of the individual's legal rights (including a private right of action, if one exists), and the legal responsibilities of the breaching organization (if any).

## **The Liberty Coalition Supports SB 728**

We urge this committee to issue a favorable recommendation to SB 728 as written. Thank you.