



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

KEALI'I S. LOPEZ
DIRECTOR

PRESENTATION OF THE
OFFICE OF CONSUMER PROTECTION

TO THE HOUSE COMMITTEE ON CONSUMER PROTECTION & COMMERCE

AND

THE HOUSE COMMITTEE ON JUDICIARY

TWENTY-SIXTH LEGISLATURE
REGULAR SESSION OF 2012

Wednesday, February 22, 2012
2:00 p.m.

**TESTIMONY ON HOUSE BILL NO. 2047, RELATING TO INFORMATION
PROTECTION.**

TO THE HONORABLE ROBERT N. HERKES, CHAIR,
TO THE HONORABLE GILBERT S.C. KEITH-AGARAN, CHAIR,
AND MEMBERS OF THEIR COMMITTEES:

The Department of Commerce and Consumer Affairs appreciates the opportunity to testify on H.B. No. 2047, Relating to Personal Information. My name is Bruce Kim, Executive Director of the Office of Consumer Protection ("OCP"). OCP supports the intent of the bill and offers the following comments and amendments in support of the proposition that personal information collected by businesses should be protected from identity theft.

H.B. No. 2047 requires businesses to implement a "comprehensive, written

policy and procedure to prevent identity theft”, and to designate an employee “to have policy and oversight responsibility for the protection of personal information”. It further requires businesses to train all employees in the implementation of the policy and procedure to prevent identity theft. The bill mandates that businesses implement these policies and procedures by January 1, 2014.

OCP submits that the following provisions should be added to section 1 of the bill:

* * *

(4) Ensure that reasonable steps be taken to select and retain third-party service providers that are capable of maintaining appropriate safeguards over personal information consistent with this section and require the third-party service provider to implement and maintain such appropriate safeguards by contract.

(5) Ensure that any contract for the disclosure of personal information to a nonaffiliated third party require that such third party implement and maintain reasonable security measures to protect such personal information records from unauthorized access, acquisition, destruction, use, modification or disclosure.

(6) Require regular monitoring to ensure that the policies and procedures for the protection of personal information consistent with this section are operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and upgrading such policies and procedures as necessary to limit risks.

Consumers have privacy rights, including the right to be left alone. They do not want their personal information, including social security numbers and encrypted personal information on their driver’s licenses, used or disseminated by businesses without their knowledge or consent. They also have a significant interest in not

becoming a victim of identity theft through no fault of their own. Therefore, businesses should take reasonable steps to safeguard their customer's personal information.

Adopting reasonable security policies and procedures to protect their customers' personal information, and training employees on these policies and procedures should be a part of any business's DNA.

Financial and other consumer credit companies are already required to develop and implement such security measures. *See* Graham-Leach-Bliley Act (1999). The FTC adopted its Standards for Safeguarding Consumer Information Rules under the Graham-Leach-Bliley Act in 2002. *See* 16 C.F.R. § 314, *et seq.* In December 2010, the FTC issued a report entitled "Protecting Consumer Privacy in an Era of Rapid Change – Preliminary FTC Staff Report". The FTC concluded that every business that "collect[s], maintain[s], share[s], or otherwise use[s] consumer data that can be linked to a specific customer, computer or device" should adopt policies to protect this information.

First, companies should adopt a "privacy by design" approach by building protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy. Companies also should implement and enforce procedurally sound privacy practices throughout their organizations, including, for instance, assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews when developing new products and services. Such concepts are not new, but the time has come for industry to implement them systematically. Implementation can be scaled to each company's business operations. Companies that collect and use small amounts of non-sensitive consumer data should not have to devote the same level of resources to

implementing privacy programs as companies that collect vast amounts of consumer data, collect data of a sensitive nature, or engage in the business of selling consumer data.

In recognition of the need to do more, an increasing number of states have adopted legislation requiring businesses to develop and implement reasonable policies and procedures to protect personal information. *See e.g.* Cal. Civ. Code § 1798.81.5(b); ORS § 646A.622; NRS § 603A.210(1); and 201 CMR 17.03(1)(Massachusetts 2009).

OCP encourages the Consumer Protection and Commerce and Judiciary committees to adopt this measure, with the suggested amendments, for the protection of Hawaii's consumers.

Thank you for the opportunity to testify on H.B. No. 2047. I would be happy to answer any questions the members may have.



NEIL ABERCROMBIE
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

KEALI'I S. LOPEZ
DIRECTOR

TO THE
HOUSE COMMITTEES ON
CONSUMER PROTECTION AND COMMERCE
AND JUDICIARY

THE TWENTY-SIXTH STATE LEGISLATURE
REGULAR SESSION OF 2012

Wednesday, February 22, 2012
2:00 p.m.

TESTIMONY ON H.B. 2047
RELATING TO INFORMATION PROTECTION

THE HONORABLE ROBERT N. HERKES, CHAIR,
THE HONORABLE GILBERT S.C. KEITH-AGARAN, CHAIR,
AND MEMBERS OF THE COMMITTEES:

My name is Iris Ikeda Catalani, Commissioner of Financial Institutions ("Commissioner"). I appreciate the opportunity to submit comments on behalf of the Department of Commerce and Consumer Affairs ("Department") on H.B. 2047.

This measure requires that all businesses develop written policies and procedures to prevent identity theft and to insure the confidentiality and privacy of personal customer information, including medical, educational, and financial records.

Further, the bill mandates that all employees must be trained to implement the privacy safeguards and procedures.

The Department believes that protecting private consumer information is very important, especially to financial institutions. As such, federal laws were promulgated to protect the non-public private information of customers and consumers. In 1999, Congress passed the Gramm-Leach-Bliley Act. The Act regulates the privacy of non-public personal financial information in the possession of financial institutions. Its safeguards rule was designed to protect the security and confidentiality of customer information and prohibits unauthorized access to or use of financial records or information. It requires financial institutions to develop administrative, technical, and physical safeguards to protect the security and privacy of customer information. These financial institution policies state that a customer's nonpublic personal information is available to employees on a "need to know" basis.

In addition the FACTA (Fair and Accurate Credit Transactions Act) of 2003, further protected customer information held by financial institutions. All financial institutions that have FDIC insurance must have an Identity Theft Program and must conduct training of its employees on a regular basis. The federal and state and FTC share in the regulation of this law, which also includes a notification process if customer information is compromised.

The Division of Financial Institutions believes financial institutions regulated by the State under Chapter 412, Hawaii Revised Statutes, have already developed the necessary tools, policies and procedures to prevent and respond to any identity theft situations as they comply with federal laws. Consequently, these institutions should be exempt from the purview of this Bill.

However, if this bill continues to move forward, we would like to identify some conflicts in the law with the federal laws which financial institutions must comply with:

1. Training (page 2): We believe there may be unintended consequences in the training provisions; first, training for identity theft should be commensurate with the duties of the employee. For instance, in a financial institution, the financial institution may not provide ID theft training to its janitorial staff or to its information technology staff or to any staff that does not have access to nonpublic personal information of a customer. Second, financial institutions retain records of the trainings provided with a sign-in sheet which is retained by the compliance department of the financial institution along with the training materials provided to the attendees. The attendance record for the training session is not made part of the employee's personnel files. When federal and state regulators determine compliance with any regulation, we request the training materials and the training log. It would be burdensome for financial institutions to go through each employee file to determine and distinguish each employee's training records. We suggest that the language of the training be amended to say:

“(b) Every business covered by this section shall provide commensurate training to train all employees who have access to protected consumer information in the implementation of the policy and procedure to prevent identity theft. Employees shall be required to sign a form acknowledging receipt of training, and the business shall deposit each employees acknowledgment in the employee’s file retain the training materials with the training log or sign-in sheet.”

2. The federal laws also require the regulators to enforce the laws. The way regulators enforce the laws is through supervision or examination. These tools assure financial institution customers that their information is kept safe. We suggest a provision to Chapter 487J, HRS:

“Businesses shall observe the provisions of this law except to the extent preempted by applicable federal law.

Thank you for the opportunity to offer testimony on this measure. I am available to respond to any questions you might have.

**Testimony Before The House Committees On
Consumer Protection & Commerce
and the Judiciary
February 22 2012
Room 325**

H.B. 2047 Relating to Information Protection

Chairs Herkes and Keith-Agaran, Vice-Chairs Yamane and Rhoads,
and Members of the Committees:

My name is Grant "Lanai" Tabura, I am testifying today on behalf of ID Theft Solutions of America. I am testifying in **Support** of HB 2047, which requires Hawaii businesses to implement a comprehensive identity (ID) theft program by January 1, 2014.

We believe that this bill is intended to enhance the protections specified in HRS Chapter 487J, 487N and 487R as well as several Federal Laws. However, this bill provides that businesses implement a comprehensive, written policy and procedures to prevent identity theft. These policies shall include safeguards such as administrative, technical and physical safeguards designed to ensure the security or integrity of personal, medical, educational and financial information for all employees. And lastly, this bill requires that each business must train each employee in the implementation of this policy and procedure to prevent identity theft.

Let me provide you with a few facts the truly reflects on the importance of this piece of legislation, over 500 million American identities have been reported lost, stolen or exposed since January 2005 – www.PrivacyRights.org., over 400,000 DECEASED individuals opened bank accounts last year – AARP statistic., Every 3 seconds someone becomes a victim of identity theft – USA TODAY, and Revenue from identity theft has surpassed revenues from drug trafficking – Secret Service March 2007. Brining it closer to home...Several dozen members of the Hawaii host committee for the APEC Summit have received letters informing them of a possible security breach involving their personal information...249,000 victims of ID theft from the University of Hawaii due to a negligent employee...and 2,000 victims of a hacker at Punahou School.

These facts become increasingly more important when we find that "Over half of all ID theft breaches happen with the work environment and that ID theft is not just financial. Financial ID theft makes up only 23% of all theft cases. Thieves are now targeting information like your SSN, Birth date, etc., information that can then be used to extract more information from a company.

These are all scary facts and reasons why we believe that this is the first step towards the protection needed for everyone in Hawaii.

We do understand that attorneys and business organizations have concerns regarding the implementation of this bill. They believe that there needs to be further clarifications or additional details in respect to: a) identification of which company employees should be trained; b) how much training should be given; and c) the identification of records that should be safeguarded, length of period that they need to be safeguarded or whether this legislation is designed to protect records that exist today or other future identification records. We would be more than willing to work with these organizations in working out these specifics although we believe that they are identified under pre-existing State and Federal Laws.

Thank you for allowing me to testify and express my **SUPPORT** for HB 2407.

GOODSILL ANDERSON QUINN & STIFEL

A LIMITED LIABILITY LAW PARTNERSHIP LLP

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

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
meito@goodsill.com
ckaramatsu@goodsill.com
ahoriuchi@goodsill.com

TO: Representative Robert N. Herkes
Chair, Committee on Consumer Protection & Commerce
Representative Gilbert S.C. Keith-Agaran
Chair, Committee on Judiciary
Via Email: CPCtestimony@Capitol.hawaii.gov

FROM: Mihoko E. Ito

DATE: February 20, 2012

RE: **H.B. 2047 – Relating to Information Protection**
Hearing Date: Wednesday, February 22, 2012 at 2:00 p.m.
Conference Room 325

Dear Chairs Herkes & Keith-Agaran and Members of the Committees:

I am Mihoko Ito with Goodsill Anderson Quinn & Stifel, submitting testimony on behalf of the Consumer Data Industry Association (CDIA). Founded in 1906, CDIA is an 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.

CDIA **submits comments** on H.B. 2047, which by January 1, 2014, requires businesses to implement a comprehensive, written policy and procedure to prevent identity theft, and to designate an employee to be responsible for protecting personal information. It further requires businesses to train all employees in the implementation of the policy and procedure.

CDIA is concerned that the measure expands the existing law in a way that will create significant additional burdens on businesses. While we understand that this measure is intended to implement a security policy to prevent identity theft, existing protections and penalties under federal and state law already exist. Federal and state laws require the private sector to maintain safe and secure databases and data transfers. State laws also require the private sector to provide for file freezing and security breach notification. Based upon the foregoing, expanding the law at this time appears to be unjustified.

We respectfully request that the foregoing concerns be considered, and welcome any questions you have regarding our comments.

Thank you very much for the opportunity to submit testimony on this measure.

Representative Robert Herkes, Chair
Representative Ryan Yamane, Vice Chair
Committee on Consumer Protection & Commerce

Representative Gilbert Keith-Agaran, Chair
Representative Karl Rhoads, Vice Chair
Committee on Judiciary

HEARING Wednesday, February 22, 2012
 2:00 pm
 Conference Room 325
 State Capitol, Honolulu, Hawaii 96813



RE: H2047, Relating to Information Protection

Chairs Herkes and Keith-Agaran, Vice Chairs Yamane and Rhoads, and 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 recognizes the intent of this proposed legislation, which by January 1, 2014, requires businesses to implement a comprehensive, written policy and procedure to prevent identity theft, and to designate an employee to be responsible for protecting personal information, and to train all employees in the implementation of the policy and procedure.

However, this legislation is not necessary. All the guidelines that businesses need to protect both employees' and consumers' personal identification already are in place. Since 2007, Sections 487N, Security Breach of Personal Information, 487R, Destruction of Personal Information Records; and 487J, Social Security Number Protection, Hawaii Revised Statutes, have provided the framework for businesses to address these issues. Additionally, there are federal laws that provide additional tiers of protection: Health Information (HIPPA); Credit and Background Checks (The Fair Credit Reporting Act); Search of Company and Employee Property; Surveillance and Electronic Monitoring of Employees (ECPA -"The Wire Tap Act" and The Stored Communications Act (SCA).

Recognizing that electronic payment systems were an area of vulnerability for the retail industry, Payment Card Identity Data Security Standard (PCI DSS) was launched in 2007. Although not a federal law, PCI applies to all organizations or merchants, regardless of size or number of transactions, that accept, transmit or store any card holder data, and defines the cardholder data that is relevant and necessary for normal operations and that which is sensitive authentication data which is prohibited. Compliance with PCI DSS is mandatory. Standards can found at this website: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Should this committee decide to advance this measure, we respectfully request considering the following:

- This requirement under §487J should be expanded to include government agencies as well; the standard should be equally applied.
- The requirement in subsection (b) to train **all** employees will be very costly and is not warranted. Employees with access to customers' payment information at POS stations are trained in policies and procedures. Employees with no such contact do not need training.
- While this mandate is another cost burden for business, we especially are concerned with the many small business owners who have neither the cash nor the time resources to comply. We suggest that perhaps DCCA could develop a template that would facilitate compliance without a major hardship.

We look forward to continuing the dialogue to develop effective and manageable regulations. Thank you for the opportunity to comment.

Carol Pregill, President

RETAIL MERCHANTS OF HAWAII
1240 Ala Moana Boulevard, Suite 215
Honolulu, HI 96814
ph: 808-592-4200 / fax: 808-592-4202



TEL:
808-524-5161
FAX:
808-521-4120
ADDRESS:
1000 Bishop Street, Suite 301B
Honolulu, HI 96813-4203

Presentation To Committees on Consumer Protection & Commerce and Judiciary
Wednesday, February 22, 2012, at 2:00 p.m.
Testimony on HB 2047 Relating to Information Protection

In Opposition

TO: The Honorable Robert N. Herkes and Gilbert S.C. Keith-Agaran, Chairs
The Honorable Ryan I. Yamane and Karl Rhoads, Vice Chairs
Members of the Committees

I am Gary Fujitani, Executive Director of the Hawaii Bankers Association (HBA), testifying in opposition to HB 2047. HBA is the trade association representing FDIC insured depository institutions with branches in Hawaii.

HB 2047 requires Hawaii businesses to implement a comprehensive identify (ID) theft program by January 1, 2014.

While the intent of this bill is laudable, we respectfully ask that the respective committees hold this bill because of the regulatory burden and cost that will be placed on the business community, especially, small businesses.

The mandate to train "**all**" employees, Section I (b), is an overreaching and costly requirement. This places unnecessary cost to train even employees that do not have access to personal information. Further the bill stipulates **only businesses** meet the new Section I ID theft ID program requirements. Hopefully, it was not the intent to only cover businesses and exclude government agencies.

During these tough economic times many business are already struggling to survive and do not need well intended, but, more regulations that may not achieve its intent. Unnecessary, but, well intended laws, only add more expenses for business, which can affect businesses' ability to retain or hire employees.

We note that previously the Legislature recognized that banks and credit unions were already subject to stringent identity theft provisions under federal law as a result of the Gramm-Leach-Bliley Act of 1999 and resulting regulations and thus, provided an exemption for banks with respect to Acts 135 and 136, Session Laws of Hawaii 2006, so that financial institutions would not be subject to duplicative but conflicting obligations.

Thus, if the committees decide to report this bill favorably, we request that financial institutions be exempt from the provisions of this bill in the same manner as under Acts 135 and 136. We would suggest that this language from HRS section 487N-2(g) (I) [Act 135] **be used to exempt financial institutions:**

"A financial institution that is subject to the Federal Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Customer Notice published in the Federal Register on March 29, 2005 by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, or subject to 12 C.F.R. Part 748, and any revisions, additions, or substitutions relating to said interagency guidance" shall be exempt from this Chapter.

Thank you for the opportunity to testify.

A handwritten signature in black ink, appearing to read 'Gary Fujitani', with a horizontal line extending to the right.

Gary Fujitani
Executive Director

**Testimony before the
House Committees on
Consumer Protection and Commerce
and Judiciary**

H.B. 2047 -- Relating to Information Protection

**Wednesday, February 22, 2012
2:00 pm, Conference Room 325**

**By Thomas Overman
Information Assurance Manager
Hawaiian Electric Company, Inc.**

Chairs Herkes and Keith-Agaran, Vice-Chairs Yamane and Rhoads and Members of the Committees:

My name is Thomas Overman. I am the Information Assurance Manager for Hawaiian Electric Company. I am testifying on behalf of Hawaiian Electric Company and its subsidiary utilities, Maui Electric Company and Hawaii Electric Light Company.

We oppose H.B. 2047 because of the lack of clarity on training, record keeping, auditing, and because of the cost of implementing the recordkeeping process required by these bills.

H.B. 2047 strives to enhance the protections specified in Chapter 487J, 487N and 487R of Hawaii Revised Statutes, which is not a bad thing per-se. This bill, however, would create a requirement for all businesses to keep records, but would not provide guidance on the length of time the records must be kept, the form and format of these records, which government agency would review/approve these records, or for whatever other purpose the records would serve. The same is true of the training requirement. It is unclear whether the State will subsequently have one of its agencies start defining the training requirements and recordkeeping formats for this bill, or whether a cottage industry

of sorts will spring up to provide this training. More importantly, it does not provide clarity on what constitutes sufficient employee training. A company might have a one-minute training which instructs employees to comply with Hawaii law, while another company might have a half-day training class giving the details and process for ensuring the intended protections. As it currently reads, both companies would be in compliance with the law, yet the training provided by these two companies would be very different. The ability for companies to be compliant with H.B. 2047, without actually providing any details in their training, would prove fatal to its ability to serve its intended function.

Another challenge is that, H.B. 1788, which is currently under consideration in the House, provides a new term called "Identifying information" which is proposed for inclusion in Chapter 708 of Hawaii Revised Statutes. The bills under consideration here do not provide guidance on whether the training should be specified toward the protections existing today in Chapter 487, or whether the training should also include the definitions of "Identifying Information" provided in H.B. 1788.

Lastly, this legislation requires privacy training of all employees regardless of their job requirements. Many of our employees do work with privacy information on a regular basis. In particular this is true of our Customer Service and Human Resources department staffs. However, we have more than a thousand employees, including electrical engineers, transmission line maintenance personnel, and power plant control operators, who have no such duties. This proposed law, as written, levies the same requirement for all types of employees, which will increase the cost of doing business here in Hawaii with a questionable return on that investment.

As stated earlier, while we support the intent of the legislation – enhancing the protections of either "Personal Information" or "Identifying Information", or both -- the ambiguities on the level of training and recordkeeping, as well as the costs of implementing such a recordkeeping process for companies, and for the State, suggest this legislation should be held.

Thank you for the opportunity to testify.

TESTIMONY OF THE AMERICAN COUNCIL OF LIFE INSURERS
COMMENTING ON HOUSE BILL 2047, RELATING TO INFORMATION PROTECTION

February 22, 2012

Via e mail: cpctestimony@capitol.hawaii.gov

Hon. Representative Robert N. Herkes, Chair
Committee on Consumer Protection and Commerce
Hon. Representative Gilbert S. C. Keith-Agaran, Chair
Committee on Judiciary
State House of Representatives
Hawaii State Capitol, Room 325
415 South Beretania Street
Honolulu, Hawaii 96813

Dear Chair Herkes, Chair Keith-Agaran and Committee Members:

Thank you for the opportunity to comment on of HB 2047, relating to Information Protection.

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-five (235) ACLI member companies currently do business in the State of Hawaii; and they represent 93% of the life insurance premiums and 92% of the annuity considerations in this State. Four fraternal benefit society member companies operate in the State of Hawaii.

ACLI and its member companies recognize that their customers expect them to maintain the security of their personal information. We acknowledge that life insurers have an affirmative and continuing obligation to protect the security of their customers’ personal information and strongly support requirements for insurers to protect the security of their customers’ personal information.

Accordingly, ACLI supports requirements for businesses to have information security programs, which include administrative, technical and physical safeguards, appropriate to the size and complexity of the business and the nature and scope of its activities. Unfortunately, however, ACLI has a number of concerns with the provisions of HB 2047 as currently written.

Section 1 of the bill proposes to add a new section to Chapter 487J to require all businesses to implement a comprehensive written policy and procedure to prevent the identity theft (page 1, lines 7 and 8). First, it is unclear why only businesses are subject to this requirement, and why Hawaii government agencies are not also required to have such policies and procedures.

Moreover, the required policy and procedure must be “to prevent identity theft” (page 1, lines 7 and 8) and designed to “prevent the occurrence of any security breach” (page 1, line 18). While ACLI member companies support requirements for businesses to have appropriate security programs and policies, they are concerned that the language noted above may be construed to give rise to an unrealistic and unachievable standard - that could render every Hawaii business vulnerable to fines, penalties and litigation for any incident deemed (with the benefit of hindsight) to have been ineffective to prevent identity theft or a security breach.

Our concerns with section 1 are exacerbated by the fact that it is not clear that the required policy and procedure must only be designed to protect the personal information of Hawaii residents. This gives rise to concern that section 1 may be construed to apply to personal information of individuals other than Hawaii residents, to which we would object.

Further, bill section 1 of the bill (page 2, lines 1-3) also requires a business to train *ALL of its employees* in implementing its identity theft and prevention program. It is difficult to understand why employees who do not handle and are not exposed or have access to personal information must have this training. Moreover, the requirements that each employee formally acknowledge in writing his or her receipt of the training and that the business include the acknowledgement in the employee’s file are unnecessary to assure a business’s employees’ knowledge of its identity theft prevention program and unnecessarily prescriptive.

To be clear, ACLI member companies do not object to requirements that a business be responsible for training its employees that have access to its customers’ personal information and to have a record of such training. However, in view of the fact that many ACLI member companies are likely to have thousands of employees, it is the requirements that each employee sign an acknowledgment of training and that the business file the acknowledgement in each employee’s file that are objectionable. We respectfully submit that these requirements would impose an unnecessary administrative burden and cost on businesses, without commensurate enhanced consumer protection.

In addition to the above, section 4 of the bill (page 3, lines 5-10) would amend §487J-5 to require a designated individual to be responsible to “ensure” compliance with the requirements of Chapter 487J (relating to personal information), 487N (dealing with security breach) and 487R (relating to destruction of personal information records). Again, we are concerned that the language noted above may be construed to give rise to an unrealistic and unachievable standard – particularly for a single individual. In fact, we are generally concerned that all the obligations imposed under subsection (b) of §487J-5 may be construed to be imposed on a single designated employee.

We also are concerned by the ambiguities likely to arise as a result of the requirement in subsection (b)(1) of §487J-5 (again at page 3, lines 5-10) to “ensure and coordinate” compliance with Chapter 487J (relating to personal information), 487N (relating to security breach) and 487R (relating to the destruction of personal information records) and how this reference might impact the application of the penalty provisions of these three chapters.

ACLI is willing to work with the legislative sponsor of the bill and all other interested parties in resolving our concerns with the bill's provisions, as described above.

Again, thank you for the opportunity to comment on HB 2047.

LAW OFFICES OF
OREN T. CHIKAMOTO
A Limited Liability Law Company



Oren T. Chikamoto
737 Bishop Street, Suite 2100
Honolulu, Hawaii 96813
Telephone: (808) 531-1500
Facsimile: (808) 531-1600



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



Testimony to the House Committee on Consumer Protection and Commerce
And the House Committee on Judiciary
Wednesday, February 22, 2012

Testimony in opposition to HB 2047, Relating to Information Protection

To: The Honorable Robert Herkes, Chair
The Honorable Ryan Yamane, Vice-Chair
The Honorable Gil Keith-Agaran, Chair
The Honorable Karl Rhoads, Vice-Chair
Members of the Committees

My name is Stefanie Sakamoto, and I am testifying on behalf of the Hawaii Credit Union League, the local trade association for 81 Hawaii credit unions, representing approximately 811,000 credit union members across the state.

We are in opposition to HB 2047, Relating to Information Protection. While we fully understand the reasons behind legislation such as this, and agree that protection of personal information with respect to identity theft prevention is of great importance, we believe this bill is unnecessary for financial institutions. There are already federal laws and regulations in place for financial institutions regarding identity theft and information protection, of which Hawaii credit unions are in full compliance.

Accordingly, we agree with the exemption for financial institutions proposed by the Hawaii Bankers Association.

Thank you for the opportunity to testify.