TESTIMONY OF THE STATE ATTORNEY GENERAL
TWENTY-FOURTH LEGISLATURE, 2008

ON THE FOLLOWING MEASURE:
S.B. NO. 2803, S.D. 1, RELATING TO PERSONAL INFORMATION.

BEFORE THE:
SENATE COMMITTEE ON WAYS AND MEANS

DATE: Monday, February 25, 2008 **TIME:** 10:30 AM
LOCATION: State Capitol, Room 211
Deliver to: Committee Clerk, Room 210, 1 copy

TESTIFIER(S): WRITTEN TESTIMONY ONLY
(For more information, contact James C. Paige, Deputy Attorney General, at 586-1180.)

Chair Baker and Members of the Committee:

The Attorney General opposes the placement of the Information Privacy and Security Council ("council") within the Department of the Attorney General.

This bill implements the recommendations of the Identity Theft Task Force. The task force did not recommend placement of the council within the Department of the Attorney General. The task force recommended that the council be administratively attached to a different department. That department, which is special funded, testified that the council would be more appropriately placed in a department that receives general funds. The Department of the Attorney General is not the appropriate place for the council. The extensive duties relating to both civil and criminal matters that are required of the Department of the Attorney General under chapter 28 of the Hawaii Revised Statutes are inconsistent with expending limited resources to house and administratively support a separate state entity. While the Department of the Attorney General advises numerous boards and commissions, and would be available to advise the council, that is entirely different from being required to provide support staff and facilities to an entity that serves an important but different purpose than the department. Accordingly, it would be difficult for the

Department of the Attorney General to provide administrative support to the council without impacting the department's priorities as detailed in our executive biennium budget. We therefore ask that the bill be amended to remove the provisions that place the council within the Department of the Attorney General.

Date of Hearing: February 25, 2008

Committee: Senate Ways and Means

Department: Education

Person Testifying: Patricia Hamamoto, Superintendent

Title: S.B. 2803, S.D.1 (SSCR2388), Relating to personal information

Purpose: To implement recommendations of the 12/2007 report of the Hawaii identity theft task force to protect the security of personal information collected and maintained by state and county government.

Department's Position: The Department of Education (Department) supports improving the security and protection of personal information collected and maintained by the State and counties. As a member of the task force, the Department recognizes the need for security measures to be enforced to protect personnel information. The Department has initiated several measures outlined by the report and will continue to enhance our existing technology and personnel management system. The Department is in agreement with the amendments cited in S.B. 2803, S.D. 1 (SSCR2388).

Testimony to the Twenty -Fourth State Legislature, 2008 Session
Senate Committee on Ways and Means
The Honorable Rosalyn H. Baker, Chair
The Honorable Shan S. Tsutsui, Vice Chair

Monday, February 25, 2008, 10:30 ap.m.
State Capitol, Conference Room 325

by

Thomas R. Keller
Administrative Director of the Courts

WRITTEN TESTIMONY ONLY

Bill No. and Title: Senate Bill No. 2803, S. D. 1, Relating to Personal Information.

Purpose: The purpose of Senate Bill No. 2803 is to implement the recommendations of the December 2007 report of the Hawaii identity theft task force to protect the security of personal information collected and maintained by state and county government.

Judiciary's Position:

The Judiciary supports the intent of this bill. Senate Bill No. 2803, S.D.1 establishes a comprehensive plan for the security of social security numbers and other personal information maintained by state government agencies. The Judiciary recognizes the need to protect against identity theft, and has already taken the initiative to implement practices similar to some procedures described in the bill.

The Judiciary submits the following comments on Sections 9, 10, 14 and 15 of the bill:

Section 9 requires that government contracts for the performance of support services by third party vendors include provisions relating to the protection of personal information. The term "support services" may be too broad. There are many contracts, such as equipment maintenance or staff training, that may be considered support service contracts, but do not require the vendor to have access to personal information. Unless "support services" is further defined, there may be confusion on whether provisions for protecting personal information must be included in all support service contracts, even when the vendor does not have access to personal information.

Section 9 also specifies the types of provisions that must be in the contract. Many vendors have comprehensive security policies that may not necessarily include all of the provisions required by the bill. Yet, these policies are adequate for the services to be provided under the contract. The bill should establish guidelines, rather than requirements, for security provisions in government contracts. This approach would give agencies and vendors the flexibility to negotiate specific conditions, applicable to their particular contract, for the protection of personal information.

Section 10 of the bill requires agencies to develop and implement plans to protect and redact personal information before disclosing documents within the scope of Hawaii Revised Statutes (HRS) section 92F-12. HRS chapter 92F, however, includes provisions that prevent disclosure of personal information. HRS section 92F-14(b) lists the types of information, including social security numbers, in which individuals have a significant privacy interest. Pursuant to HRS section 92F-13(1), information in which individuals have a significant privacy interest is not subject to disclosure. The Judiciary's experience, both internally and with other agencies, is that government agencies are familiar with the provisions of HRS sections 92F-13 and 92F-14. Personal information is routinely redacted before government records are made available for public inspection.

Section 14 requires that agencies with primary responsibility for human resource functions develop recommended practices to minimize unauthorized access to personal information in various areas, such as personnel recruitment and payroll. The recommended practices must also include technical safeguards to ensure confidentiality of electronically transmitted information.

Human resource staff do not necessarily have the expertise to develop recommended practices in all of the areas described in Section 14. For example, human resource personnel do not have the expertise to make recommendations on best practices to safeguard electronically transmitted information. This section should provide agency heads and directors with more flexibility to designate the appropriate personnel to develop recommended practices.

Section 15 requires government agencies to develop written policies on notification of security breaches of personal information, including contents of the notification and manner in which notification shall be provided. This section duplicates HRS chapter 487N, which establishes legal requirements that government agencies must comply with in the event of a security breach of personal information.

Thank you for the opportunity to testify on Senate Bill No. 2803, S. D.1.

Senator Roslyn Baker, Chair
Senator Shan Tsutsui, Vice Chair
Committee on Ways and Means
State Capitol, Honolulu, Hawaii 96813

HEARING Monday, February 25, 2008
10:30 am
Conference Room 211

RE: SB2803, SD1, Relating to Personal Information

Chair Baker, Vice Chair Tsutsui, and Members of the Committee:

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 support the retail industry and business in general in Hawaii.

RMH supports SB2803, SD1, which implements the recommendations of the Identity Theft Task Force.

As a member of the Identity Theft Task Force, representing retail and the small business community, I was enlightened and sometimes appalled with the complexity of the issues and the gravity of the concerns of government and private industry. SB2803, SD1 provides recommendations, guidelines and best practice solutions that will help us all accomplish our goals.

Thank you for your consideration and for the opportunity to comment on this measure.

Carol Pregill
President

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

GOODSILL ANDERSON QUINN & STIFEL

A LIMITED LIABILITY LAW PARTNERSHIP LLP

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

GOVERNMENT RELATIONS TEAM:
GARY M. SLOVIN, ESQ.
CHRISTOPHER G. PABLO, ESQ.
ANNE T. HORIUCHI, ESQ.
MIHOKO E. ITO, ESQ.
JOANNA J. H. MARKLE*
LISA K.KAKAZU**
* Government Relations Specialist
** Legal Assistant

INTERNET:
gslovin@goodsill.com
cpablo@goodsill.com
ahoriuchi @goodsill.com
meito@goodsill.com
jmarkle@goodsill.com
lkakazu@goodsill.com

February 23, 2008

TO: Senator Rosalyn Baker
Chair, Senate Committee on Ways and Means
Hawaii State Capitol, Room 210

Via Email: testimony@Capitol.hawaii.com

FROM: Joanna Markle

RE: S.B. 2803, SD1 – Relating to Personal Information
Hearing Date: Monday, February 25, 2008 @ 10:30 a.m., Room 211

Dear Chair Baker and Members of the Committee on Ways and Means:

I am Joanna Markle testifying on behalf of the Consumer Data Industry Association. Founded in 1906, the Consumer Data Industry Association (CDIA) is the international trade association that represents more than 400 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening and collection services.

CDIA opposes part VI of S.B. 2803, SD1. S.B. 2803, SD1 is intended to implement the recommendations of the December 2007 report of the Hawaii Identity Theft Task Force to protect the security of personal information collected and maintained by state and county governments. CDIA applauds the time and efforts of the members of the Hawaii Identity Theft Task Force. As an observer at these meetings, it was clear that this was a very large task to undertake in such a short period of time.

However, with regard to Parts V, VI, and VII, we urge the legislature and the government agencies to carefully consider the unintended negative consequences of limiting access to and/or collection of Social Security numbers. Consumer reporting agencies use several key pieces of identifying information to match a public record to a credit file, but the only piece of identifying information that is unique to the individual is the Social Security number. Every other element - name, address, date of birth - changes and/or is not unique. The full Social Security number is critical to identifying a person.

Consumer reporting agencies take great effort to ensure that the information they provide is accurate, current and complete. In fact, the Fair Credit Reporting Act requires a consumer

reporting agency to have reasonable procedures "to assure maximum possible accuracy of the information concerning the individual about whom the report relates" (15 USC Section 1681(e)(a)). The full Social Security number is critical to accurately match the public record to the correct credit file. While truncating a Social Security number so that only the last four numbers are available may sound like a compromise, surprisingly very few additional records can be matched to the exacting standards imposed by law on agencies using only truncated numbers. The benefit of truncation is marginal. The harm caused by being unable to verify information is substantial.

Fraudsters rarely use public records to perpetrate identity fraud because there is not enough information even in a record that contains a full Social Security number. In fact, a public record with a full Social Security number can help prevent identity theft because it provides an authentic record against which a fraudulent application could be challenged. While it may seem counter-intuitive, the response to fraud relies on more information, not less. Redaction of SSNs or limiting access to SSNs for consumer reporting agencies will have serious consequences.

CDIA believe there may well be severe consequences to truncating or eliminating the use of social security numbers in public records. Criminal background checks will not be as effective. The consequences of a person with a criminal past getting through such a check could well be very harmful. Persons committing fraud would benefit from this as credit checks could not be as effective. These severe consequences need to be balanced against the questionable benefits of diluting the effect of social security numbers. CDIA knows its position is not a popular one but the effort to prevent ID theft needs to be balanced against these unintended consequences.

Part VI is especially troubling because it directs all government agencies to develop and implement a plan to protect and redact personal information, specifically social security numbers, contained in any existing hardcopy documentation. We would respectfully ask for consideration in exempting the information given to consumer reporting agencies governed under the FCRA. To illustrate why CRAs must have the full SSN to ensure that its customers, including preschools, senior care homes, financial institutions, have the information they need to ensure the safety and the interests of the people they serve, we would like to share the following:

In September 2003, a national CDIA member performed a test using 9,906 bankruptcy records. This company ran a test with and without the SSN. With an SSN, name and full or partial address (some court records were missing city, state or zip information) the company was able to accurately match 99.82% of the records. Without the SSN, 25.71% failed an identification/authentication match (6.11% were due to an incomplete address/no SSN and an additional 19.60% failed due to the lack of an SSN).

The company also conducted an analysis using the last four digits of the SSN in identifying the correct consumer. According to the company "searching our database on only the last 4 digits

identifies too many possible false-positive candidate consumers to be evaluated. Therefore we had to omit this search option and consequently miss any consumer matches that the 9 digit SSN would provide."

Using the 4 digit SSN in the company's match evaluation was also analyzed. The following is an anonymous example of an actual search:

> Record: Chapter 7 bankruptcy for Juan Gonzales, 100 Main St., Orange CA, SSN XXX-XX-4587.
>
> On file data:
> Juan B. Gonzales, 100 Main St, Orange, CA, SS XXX-XX-4587
> Juan R. Gonzales, 100 Main St, **Apt 22**, Orange, CA SS XXX-XX-458**9**
> Juan Gonzales, **2**01 Main St, Orange, CA SS XXX-XX-4587
> Juan B. Gonzales, 100 Main St, Orange, CA SS XXX-XX-4**8**87

CDIA is committed to addressing identity theft, which is why we worked very hard in 2006 to pass measures to establish laws on destruction of personal records, security breaches, and file freezing. However, Part VI of S.B. 2803, SD1 will not serve the purpose of protecting people from identity theft and for this reason, we urge you to delete this section and allow the Information Privacy and Security Council created by this bill to focus on effective methods of battling identity theft, such as education of consumers and adoption of strict policies and procedures regarding handling of personal information.

S.B. 2803, SD1 creates an Information Privacy and Security Council and we would suggest that the issue of SSNs be further researched and considered by this council.

Thank you for the opportunity to testify.

HAWAII FINANCIAL SERVICES ASSOCIATION

c/o Marvin S.C. Dang, Attorney-at-Law
P.O. Box 4109
Honolulu, Hawaii 96812-4109
Telephone No.: (808) 521-8521
Fax No.: (808) 521-8522

February 25, 2008

Senator Rosalyn H. Baker, Chair,
and members of the Senate Committee on Ways & Means
Hawaii State Capitol
Honolulu, Hawaii 96813

Re: **Senate Bill 2803, Senate Draft 1 (Personal Information)**
Decision-Making Date/Time: Monday, February 25, 2008, 10:30 A.M.

I am the attorney for the Hawaii Financial Services Association ("HFSA"). The HFSA is the trade association for Hawaii's financial services loan companies.

The HFSA **supports** this Bill.

The purpose of this Bill is to implement recommendations of the December 2007 report of the Hawaii Identity Theft Task Force to protect the security of personal information collected and maintained by the State and County governments. The December 2007 Report of the Identity Theft Task Force is a continuation of the work that started with the State's Anti-Phishing Task Force which was created in 2005.

I was appointed by the Senate President to be a member of the Hawaii Identity Theft Task Force as a representative of the financial services industry. I served as Vice Chair of that Task Force. I was also a Senate President appointee of the predecessor Anti-Phishing Task Force.

The members of the Identity Theft Task Force agreed that much needs to be done within the State and County governments to protect people's personal information that exist in government records. For example, social security numbers and other personal information are easily available to the public in the Judiciary's court files and at the Bureau of Conveyances. The Report's recommendations address these concerns. Safeguarding the personal information of our citizens needs to be given a high priority.

Thank you for considering this testimony.

Marvin S.C. Dang

UNIVERSITY OF HAWAI'I SYSTEM
Legislative Testimony

Testimony Presented Before the
Senate Committee on Ways and Means
February 25, 2008 at 10:30 am
by
David Lassner
Vice President for Information Technology and Chief Information Officer
University of Hawai'i

SB 2803, SD 1 – RELATING TO PERSONAL INFORMATION

Chair Baker, Vice Chair Tsutsui and Members of the Committee:

The University applauds the Legislature's concern in protecting Hawaii's citizenry. While we oppose several provisions of the proposed legislation in its current form for the reasons cited below, we appreciate the thoughtful consideration of our concerns by the Committees on Economic Development & Taxation and Judiciary & Labor. We support their recommendation to delay implementation of this Bill until such time as the remaining issues can be thoughtfully addressed.

In the spirit of supporting improved protection of personal information held in the public sector, the University offers the following specific comments:

1) The University strongly opposes the creation of the Annual Report on Systems with Personal Information (proposed as §487N-C). The very creation of such a report creates significant new risks for Hawaii's citizens by establishing a convenient "one-stop shop" for interested hackers and criminals who are targeting personal information in Hawai'i. Any perceived value in creating such a report is more than outweighed by the new risks created by a new public record that tells criminals exactly where to find personal information and what is in each location.

   The University would suggest that the current provisions be replaced with more general language that simply specifies that each agency, in support of their internal programs of protection of personal information, shall be responsible to maintain an inventory of all information systems that include personal information. The legislation must ensure that any such inventories remain confidential and fully protected from disclosure notwithstanding any other rules or statutes.

2) They University strongly opposes the provisions in Part VII that would require the elimination of all governmental uses of Social Security Numbers other than where required by law. While we no longer use the Social Security Number as a

primary identifier in any of our information systems, the fact remains that the Social Security Number was the identifier in the past and is still an important element in establishing identity. The University would have no way of establishing the identities of hundreds of thousands of our past students without the use of the Social Security Number, which was formerly used as the Student ID number.

The Social Security Administration notes that:

> *"The Privacy Act regulates the use of Social Security numbers by government agencies. When a federal, state, or local government agency asks an individual to disclose his or her Social Security number, the Privacy Act requires the agency to inform the person of the following: the statutory or other authority for requesting the information; whether disclosure is mandatory or voluntary; what uses will be made of the information; and the consequences, if any, of failure to provide the information."*

The University urges that the legislature not frustrate our ability to serve our customers throughout the state with overly restrictive legislation that goes so far beyond the federal requirements and Social Security Administration guidelines.

3) The University notes that a number of new compliance mandates are established in the current draft without specific funding. While the bill invites agencies to prepare budget requests for addressing certain requirements, we hope that the final bill will link compliance with the appropriation and release of the funding the Legislature recognizes will be necessary.

Finally, the University notes that while government agencies, including the University, must protect the personal information with which they are entrusted, a singular focus on governmental protection of personal data is a small part of protecting the public against identity theft. National data tells us that:

- More personal data is lost by the private sector that the public sector;
- Most identity theft is not the result of data breaches; and
- Most losses of personal data do not result in identify theft.

True protection against identity theft will only occur with changes in the credit industry, which is where the crime actually occurs. This is of course a much more difficult target for reform.

Nonetheless, the University takes the protection of the personal information with which we are entrusted very seriously, and looks forward to working with the Legislature to craft legislation that will reduce risks for Hawai'i's citizenry.