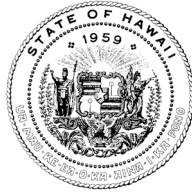


DAVID Y. IGE
GOVERNOR



DOUGLAS MURDOCK
CHIEF INFORMATION
OFFICER

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

P.O. BOX 119, HONOLULU, HI 96810-0119
Ph: (808) 586-6000 | Fax: (808) 586-1922
ETS.HAWAII.GOV

Testimony of
DOUGLAS MURDOCK
Chief Information Officer
Enterprise Technology Services

Before the

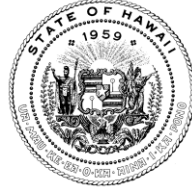
SENATE COMMITTEE ON JUDICIARY
MONDAY, FEBRUARY 28, 2022

SENATE BILL NO. 2292 SD1
RELATING TO PRIVACY

Dear Chair Rhoads, Vice Chair Keohokalole, and members of the committee,

The Office of Enterprise Technology Services supports updating the definition of “personal information” in HRS Section 487N to add expanded identifiers and data elements that many other states have included in their security breach notification laws. These changes recognize many new identifying data elements that have been created since Hawaii enacted that statute in 2008.

Thank you for the opportunity to provide testimony on this measure.



DAVID Y. IGE
GOVERNOR

JOSH GREEN
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
cca.hawaii.gov

CATHERINE P. AWAKUNI COLÓN
DIRECTOR

JO ANN M. UCHIDA TAKEUCHI
DEPUTY DIRECTOR

Testimony of the Department of Commerce and Consumer Affairs

**Before the
Senate Committee Judiciary
Monday, February 28, 2022
10:30 a.m.
State Capitol, Videoconference**

**On the following measure:
S.B. 2292, S.D. 1, RELATING TO PRIVACY**

Chair Rhoads, and Members of the Committee:

My name is Stephen Levins, and I am the Executive Director of the Department of Commerce and Consumer Affairs' (Department) Office of Consumer Protection (OCP). The Department supports this bill with amendments as referenced in this testimony.

The purpose of this bill is to modernize the definition of "personal information" for the purposes of notifying affected persons of data and security breaches.

The Department supports S.B. 2292, S.D. 1's expansion of the definition "personal information" in Hawaii Revised Statutes (HRS) chapter 487N because the current definition is obsolete. Businesses that collect or store data digitally have a responsibility to protect information that is sensitive, confidential, or identifiable from access by hackers; these businesses also have a responsibility to prevent the data from being made available to criminals who engage in identity theft. As of 2018, all 50 states have data breach notification laws that prescribe when consumers must be notified

when their “personal information” has been breached. Hawaii’s data breach notification laws were codified in 2006 as HRS chapter 487N, which, in pertinent part, defines “personal information” in relation to when a breach notification is required, and specifies the circumstances in which a business or government agency must notify a consumer that his or her personal information has been breached. Although Hawaii was one of the first states to enact this law, advancements in technology have made identity theft easier than it was 16 years ago. Businesses and government agencies now collect far more information, and bad actors exploit vulnerabilities in computer databases for nefarious purposes and with increased frequency.

However, the Department believes the language in the original draft was far more protective of privacy and therefore requests that it be reinserted. The original bill corrected existing statutory inadequacies by expanding the definition of “personal information” to include various personal identifiers and data elements, such as email addresses, health insurance policy numbers, security codes, and medical histories. This would enhance consumer protections involving privacy and align with legislation recently enacted in other jurisdictions, including Vermont and California.

The Department prefers the original language of the bill because it provides broader protection:

“Identifier” means a common piece of information related specifically to an individual, that is commonly used to identify that individual across technology platforms, including a first name or initial, and last name; a user name for an online account; a phone number; or an email address.

“Specified data element” means any of the following:

(1) An individual's social security number, either in its entirety or the last four or more digits;

(2) Driver's license number, federal or state identification card number, or passport number;

(3) A federal individual taxpayer identification number;

(4) An individual's financial account number or credit or debit card number;

(5) A security code, access code, personal identification number, or password that would allow access to an individual's account;

(6) Health insurance policy number, subscriber identification number, or any other unique number used by a health insurer to identify a person;

(7) Medical history, medical treatment by a health care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile;

(8) Unique biometric data generated from a measurement or analysis of human body characteristics used for authentication purposes, such as a fingerprint, voice print, retina or iris image, or other unique physical or digital representation of biometric data; and

(9) A private key that is unique to an individual and that is used to authenticate or sign an electronic record."

2. By amending the definition of "personal information" to read:

~~""Personal information" means an [individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:~~

~~(1) Social security number;~~

~~(2) Driver's license number or Hawaii identification card number; or~~

~~(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.]~~

identifier in combination with one or more specified data elements. "Personal information" [~~does~~] shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."

The Department is concerned with several changes to the list of specified data elements. S.D. 1 now requires "more than the last four digits" of an individual's social security number to be considered a "specified data element". Individuals who received their social security numbers in Hawaii prior to 2004 are particularly vulnerable because the social security numbers were issued one of only two prefixes or area numbers: 575 or 576. The middle two numbers, or the group number, were also systematically allocated to the State by the Social Security Administration (SSA) and can be verified on the agency's website. For example, only 31 group numbers were issued for Hawaii residents in 1975. Hawaii residents who applied for a social security number between 2004 and 2011 were issued two area numbers: 750 and 751, and 11 group numbers. The SSA began randomizing social security numbers in June 2011 in order to make it more difficult to reconstruct social security numbers using public information. As such, the last four digits of a social security number should be included as a specified data element because the first five numbers of social security numbers issued in Hawaii prior to 2011 can easily be reconstructed.

S.D. 1 also removes an individual's medical history as a specified data element. The Department believes that medical history is an important data element because it is information that can be easily linked to an individual. For instance, hacked medical records containing the medical history of an individual can provide enough information to identify, trace, or locate a person.

It is a common misconception that the Health Insurance Portability and Accountability Act (HIPAA) applies to the maintenance of all health records. On the contrary, HIPAA only applies to "covered entities." For instance, HIPAA generally does

not apply to employee health information maintained by an employer. Even when HIPAA applies to an entity, it does not apply to **all** health information held by the entity. It would apply only to information held in the context of the health care or other functions that make the entity a Covered Entity or Business Associate. The organizations that are required to follow HIPAA rules and regulations include health plans, most healthcare providers and healthcare clearinghouses. Organizations that do not have to follow HIPAA include life insurers, employers, worker's compensation carriers, most schools and school districts, state agencies, law enforcement, and municipal offices.

S.D. 1 corrects existing statutory inadequacies by expanding the definition of "personal information" to include various personal identifiers and data elements, such as email addresses, health insurance policy numbers, security codes, and medical histories. The measure also subjects the business associates of health plan or health care providers to the same security standards for securing electronic health information according to the Health Insurance Portability and Accountability Act of 1996. Expanding the definition of "personal information" will enhance consumer protections involving privacy and align with legislation recently enacted in other jurisdictions, including, Nevada, Rhode Island, Vermont and California.

Thank you for the opportunity to testify on this bill.

Presentation to The
Committee on Judiciary
Friday, February 28, 2022, 10:30 AM
State Capitol Conference Videoconference

Testimony on SB 2292, SD1 With Proposed Amendments

TO: The Honorable Karl Rhoads, Chair
The Honorable Jarrett Keohokalole, Vice Chair
Members of the Committee

My name is Neal K. Okabayashi, Executive Director of the Hawaii Bankers Association (HBA). HBA represents seven Hawai'i banks and three banks from the continent with branches in Hawai'i.

We are appreciative of the amendments reflected in SB 2292, SD 1. However, we think it be prudent to carefully consider the amendments proposed within.

This bill will amend the definition of "personal information" and we do not object to the substance of the bill, but we believe that the bill can be improved by including the following amendments.

On page 2, lines 15-19, we believe that the definition of "Identifier" is vague. The definition is not specific as what would be an identifier and leads to confusion as to what is an "identifier". Rather than including examples of what is an identifier, the bill should specifically state what is an identifier. A home phone number can be the number for a variety of individuals and thus should not be an identifier, although a mobile phone can be an identifier. While we think that each individual has a specific email address, a business email address is not always specific to an individual.

Using a name by first name or initial as an identifier is vague. Is the initial the middle initial or initials or the first name such as B. John Doe, and in most cases, B. John Doe goes by John Doe.

It is better to amend the definition of "Identifier" as follows on page 2, lines 15-19.

""Identifier" means a common piece of information as set forth below related specifically to an individual, that is commonly used to identify that individual across technology platforms [.] [including a first name or initial, and last name] A name used by an individual which name shall include the first name, nickname, all initials in the name, whether at the beginning of the name or middle, and the last name; a user name for an online account; a mobile phone number; or an email address specific to the individual.

On page 3, line 6 and 7, that should be amended to read as follows: "An individual's financial account number or credit or debit card number unless redacted." Credit card number are almost always redacted on a credit card receipt.

On pages 4 and, lines 20-21 and 1-2, respectively, the definition of personal information can be improved by deleting “from federal, state, or local government records”, so that it will read:

“Personal information [does] shall not include publicly available information that is lawfully made available to the public [from federal, state, or local government records], or personal information that is deidentified or aggregated so that the identity the individual is unknown.

There is no reason that the exception for publicly available information should be restricted to that made available by the government since the information could be published by the media, blog, disseminated on television, radio or podcast or otherwise. It would be difficult for a business to determine whether personal information was only made available from federal, state, or local government records.

Thank you for the opportunity to submit this testimony to offer our proposed amendments to SB 2292. Please let us know if we can provide further information.

Neal K. Okabayashi
(808) 524-5161



**Hawaiian
Electric**

**TESTIMONY BEFORE THE SENATE COMMITTEE ON
JUDICIARY**

S.B. 2292 SD1

Relating to Privacy

Monday, February 28, 2022
10:30 a.m., Agenda Item 5
State Capitol, via Videoconference

Wendee Hilderbrand
Managing Counsel & Privacy Officer
Hawaiian Electric Company, Inc.

Chair Rhoads, Vice Chair Keohokalole, and Members of the Committee,

My name is Wendee Hilderbrand, and I am testifying on behalf of Hawaiian Electric Company, Inc. (Hawaiian Electric) **in support of SB 2292, SD1**. We appreciate and support the amendment made by the previous committee, which removed medical information from the definition of “Personal Information.” Hawaiian Electric is supportive of modernizing Hawaii’s data breach statute and believes that data elements such as partial social security numbers, passport numbers, and digital signatures should be added to HRS 487N-1, as those data elements may all be used to perpetrate identity theft, which is the danger HRS 487N-1 was designed to address. Medical information, by contrast, is not used for identity theft and is otherwise protected by comprehensive federal regulation.

In light of this amendment, Hawaiian Electric is pleased to support SB 2292, SD1. 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

February 28, 2022

Senator Karl Rhoads, Chair
Senator Jarrett Keohokalole, Vice Chair
and members of the Senate Committee on Judiciary
Hawaii State Capitol
Honolulu, Hawaii 96813

Re: **S.B. 2292, S.D. 1 (Privacy)**
Decision Making Date/Time: Monday, February 28, 2022, 10:30 a.m.

I am Marvin Dang, the attorney for the **Hawaii Financial Services Association** ("HFSA"). The HFSA is a trade association for Hawaii's consumer credit industry. Its members include Hawaii financial services loan companies (which make mortgage loans and other loans, and which are regulated by the Hawaii Commissioner of Financial Institutions), mortgage lenders, and financial institutions.

The HFSA submits comments on this Bill.

This Bill modernizes the definition of "personal information" for the purposes of notifying affected persons of data and security breaches.

When this Bill was heard before the Senate Committee on Commerce and Consumer Protection on January 28, 2022, the HFSA proposed an amendment to the definition of "specified data element" regarding social security numbers.

The CPN Committee incorporated the HFSA's proposed amendment in the Senate Draft 1 version which is before your Committee.

Accordingly, the HFSA no longer has concerns about that social security number portion of the definition of "specified data element."

Thank you for considering our testimony.



MARVIN S.C. DANG

Attorney for Hawaii Financial Services Association

(MSCD/hfsa)

February 26, 2022

S.B. 2292 Relating to Privacy
Senate Committee on Judiciary
Hearing Date/Time: Friday, February 28, 2022, 10:30 AM

Dear Chair Rhoads, Vice Chairs Keohokalole, and members of the Committee:

I write in **SUPPORT** of S.B. 2292 Relating to Privacy. However, an amendment has been placed into the bill with SD1 that inadvertently lessens the protection specifically for adults raised in Hawaii. As a privacy expert, I have worked in data privacy for over 15 years and served on the 21st Century Privacy Law Task Force created by HCR 225. I have the following concern:

With SD1, this bill was changed to provide a breach notification only when more than 4 digits of SSN are compromised. The problem is that adults who were raised here, and therefore had the SSNs issued in Hawaii, have either 575 or 576 as the first 3 digits of their SSN. So if a bad actor has the last 4 digits of a local's SSN, then all that protects the person's SSN is the middle two digits. In some years, as few as 19 combinations were used for these middle 2 digits; and these combinations are publically available.

In summary, for an adult raised in Hawaii, a breach of "only" 4 digits IS THE SAME a breach of 6 digits. Please restore this aspect of the bill to the original version and protect the people who were raised in Hawaii.

Thank you for your consideration and the opportunity support this legislation.



Kelly McCanlies
Fellow of Information Privacy, CIPP/US, CIPM, CIPT



Monday, February 28, 2022 at 10:30 AM
Via Video Conference

Senate Committee on Judiciary

To: Senator Karl Rhoads, Chair
Senator Jarrett Keohokalole, Vice Chair

From: Michael Robinson
Vice President, Government Relations & Community Affairs

**Re: Testimony In Support -- SB 2292, SD1
Relating to Privacy**

My name is Michael Robinson, and I am the Vice President of Government Relations & Community Affairs at Hawai'i Pacific Health. Hawai'i Pacific Health is a not-for-profit health care system comprised of its four medical centers – Kapi'olani, Pali Momi, Straub and Wilcox and over 70 locations statewide with a mission of creating a healthier Hawai'i.

I am writing in SUPPORT of SB 2292, SD1 which updates the definition of "personal information" in chapter 487N, Hawaii Revised Statutes, to include various personal identifiers and data elements that are found in more comprehensive laws.

HPH appreciates the amendments in Section 3 of the bill that provide a carve-out for business associates of healthcare providers which are in compliance with HIPAA requirements. Pursuant to the amendments, business associates would be deemed to be in compliance with Section 487N-2, Hawaii Revised Statutes.

The outdated definition of "personal information" in chapter 487N, Hawaii Revised Statutes, which requires the public to be notified of data breaches, should be updated and expanded. Individuals face too many identifying data elements that, when exposed to the public in a data breach, place an individual at risk of identity theft or may compromise the individual's personal safety. In its current form, chapter 487N is not comprehensive enough to cover the additional identifiers. This measure is both timely and necessary to ensure individuals' privacy interests are protected.

Thank you for the opportunity to testify.

LATE



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 Senate Committee on Judiciary
Monday, February 28, 2022
10:30 am
Via Videoconference

Comments on SB 2292 SD1, Relating to Privacy

To: The Honorable Karl Rhoads, Chair
The Honorable Gil Keith Agaran, Vice-Chair
Members of the Committee

My name is Stefanie Sakamoto, and I am testifying on behalf of the Hawaii Credit Union League, the local trade association for 48 Hawaii credit unions, representing over 867,000 credit union members across the state.

We offer the following comments regarding SB 2292 SD1, Relating to Privacy. This bill would amend the definition of "personal information" for the purpose of applying modern security breach of personal information law.

While we understand the intent of this bill, we have the following comments.

This bill defines "identifier" as a "common piece of information related specifically to an individual, that is commonly used to identify that individual across technology platforms". We have concerns that "common piece of information" is too broad. The criteria of what constitutes "common" should not be left to interpretation.

Additionally, credit unions and other financial institutions are already required to safeguard sensitive data and financial information via the Gramm-Leach-Bliley Act.

Thank you for the opportunity to provide comments on this issue.