

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

HOUSE COMMITTEE ON HIGHER EDUCATION & TECHNOLOGY  
Wednesday, March 16, 2022

SENATE BILL NO. 2292 SD1  
RELATING TO PRIVACY

Dear Chair Takayama, Vice Chair Clark, 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.

## **TESTIMONY OF ALISON UEOKA**

---

COMMITTEE ON HIGHER EDUCATION & TECHNOLOGY  
Representative Gregg Takayama, Chair  
Representative Linda Clark, Vice Chair

Wednesday, March 16, 2022  
2:00 p.m.

### **SB 2292, SD1**

Chair Takayama, Vice Chair Clark, and members of the Committee on Higher Education & Technology, my name is Alison Ueoka, President of the Hawaii Insurers Council. The Hawaii Insurers Council is a non-profit trade association of property and casualty insurance companies licensed to do business in Hawaii. Member companies underwrite approximately forty percent of all property and casualty insurance premiums in the state.

Hawaii Insurers Council strongly supports the provision in this bill in Section 3, page 6, lines 4-5 that allows for an exemption for any licensee that is subject to the Insurance Data Security Law pursuant to article 3B, chapter 431.

In 2021, the Hawaii Legislature enacted the Insurance Data Security Law which is a National Association of Insurance Commissioners' (NAIC) model act. It is a comprehensive law that addresses data security and privacy issues specifically pertaining to the business of insurance, including property and casualty insurance. Therefore, the exemption contained in this bill is appropriate.

There has been testimony on this bill requesting it go back to the language in the original version of the bill. We ask that, if this committee decides to revert to language in the original bill, the exemption for licensees subject to the Insurance Data Security Law be kept intact.

Thank you for the opportunity to testify.

Wednesday, March 16, 2022 at 2:00 PM  
Via Video Conference; Room 309

**House Committee on Higher Education & Technology**

To: Representative Gregg Takayama, Chair  
Representative Linda Clark, 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.



**Hawaiian  
Electric**

**TESTIMONY BEFORE THE HOUSE COMMITTEE ON  
HIGHER EDUCATION & TECHNOLOGY**

**S.B. 2292 SD1**

**Relating to Privacy**

Wednesday, March 16, 2022  
2:00 p.m., Agenda Item 4  
State Capitol, via Videoconference

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

Chair Takayama, Vice Chair Clark, 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 in the Senate, 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.



March 15, 2022

The Honorable Greg Takayama  
Chair, House Committee on Higher Education and Technology  
Hawaii State Capitol, Conference Room 309  
Honolulu, HI 96813

The Honorable Linda Clark  
Vice Chair, House Committee on Higher Education and Technology  
Hawaii State Capitol, Conference Room 309  
Honolulu, HI 96813

**RE: SB 2292 -- Oppose**

Dear Chair Takayama and Vice Chair Clark:

On behalf of Verizon, I submit testimony in opposition to Senate Bill 2292. As drafted, the bill is problematic with over broad definitions that would create great uncertainty in implementation and create confusion for both businesses and consumers.

As currently drafted, the bill would create a data breach law for Hawaii that is not interoperable with other states, and in a matter involving transactions across the national landscape, the legislation would inadvertently make the state an outlier.

As also indicated by the industry's State Privacy Coalition, we do not object to an update of Hawaii's breach statute, but view the definitions as currently drafted as overbroad. They seek to capture information that goes beyond what actually present a risk of identity theft or other types of consumer fraud to the affected individuals. Overbroad or vague data elements mean that, in many cases, consumers will receive confusing notices that their identities may be at risk, when in reality no such risk exists. Furthermore, the bill treats publicly available information as a potential breach, which is impractical.

The "identifier" definition in the bill is very problematic. This definition would be the only one of its kind across all 50 states; for data breach notification statutes, the concept of alignment is key. In the unfortunate situation of an actual data breach, it is important to have a statute that is aligned with the other states, so that notification to state residents is fair, efficient, and consistent. Businesses will not have to segment out Hawaii residents from other states, as they will likely do if the bill advances in its current form. Much of our concern stems from the "common" nature of the information referenced in the definition, from phone numbers to email addresses, these pieces of information are widely available – even publicly available – and would dramatically

increase the scope of what could constitute a breach of security. This would be very confusing to consumers.

For these reasons, we believe that SB 2292 would have unfortunate consequences for both consumers and businesses, and we urge a “NO” vote on the legislation.

Sincerely,

Michael Bagley  
Executive Director, Government Affairs

# STATE PRIVACY & SECURITY COALITION

March 16, 2022

Chair Gregg Takayama  
House Committee on  
Higher Education & Technology  
Hawaii State Capitol, Room 404  
415 South Beretania St.  
Honolulu, HI 96813

Vice Chair Linda Clark  
House Committee on  
Higher Education & Technology  
Hawaii State Capitol, Room 303  
415 South Beretania St.  
Honolulu, HI 96813

## Re: SB2292 Amendments

Dear Chair Takayama and Vice Chair Kitagawa,

The State Privacy & Security Coalition, a coalition of 32 companies in the retail, payment card, automotive, technology, and telecom sectors (nearly all of whom serve consumers in the state of Hawaii), as well as seven trade associations, writes in opposition to SB2292, but would like to work with you to improve the legislation with several amendments that would reduce consumer confusion and align Hawaii's data breach notification requirements to be interoperable with other states.

We appreciate the legislature's work on this statute over the past several years. While we do not object to an update of Hawaii's breach statute, we do believe that the definitions as currently drafted are overbroad; they would benefit from a narrower focus on those elements that truly present a risk of identity theft or other types of consumer fraud to the affected individuals. Overbroad or vague data elements mean that, in many cases, consumers will receive confusing notices that their identities may be at risk when, in reality, no such risk exists. The amendments we offer retain the expanded list of Hawaii data elements (financial accounts, biometric information, health information, etc.) while ensuring that consumers would receive notice for events that could in fact put their identities at risk.

Our amendments are as follows:

1. **Delete the "identifier" definition:**

All other states define personal information using a "(first initial/name + last name) + data elements" formulation. We believe it makes sense for Hawaii to add new data elements reflecting a modern online ecosystem, but should not depart from the formula used by all other states by creating a new category of "identifiers".

This definition would be the only one of its kind across all 50 states; for data breach notification statutes, the concept of alignment is key. In a data breach scenario, having a statute that is aligned with other states' means that notification to state residents is far more efficient. Businesses will not have to

# STATE PRIVACY & SECURITY COALITION

segment out Hawaii residents from other states, as they will likely do if the bill advances in its current form.

Much of our concern stems from the “common” nature of the information referenced in the definition, from phone numbers to email addresses, these pieces of information are widely available – even publicly available – and would dramatically increase the scope of what could constitute a breach of security. This would be very confusing to consumers. As an example, if a hacker obtains an individual’s unencrypted driver’s license number, it is likely not an increased indicator of risk for that person to have a phone number as well.

To address the issue of unauthorized account access, we offer a solution in our fourth point, below.

2. **Recognize the value of encrypted or unusable information:** This is important to avoid consumer confusion and align with other states. Specifically, when information is accessed in an unauthorized manner, there is likely no risk to a Hawaii resident if the information is encrypted or otherwise protected and the hacker does not also have the encryption key. No other state defines a breach of security to include encrypted or otherwise protected information, and Hawaii should not deviate from this practice. From the consumer’s viewpoint, requiring breach notifications for encrypted or unusable information would result in misleading notices, leading them to believe that their information was available to hackers or cybercriminals, when this was in fact not the case. Additionally, it will further encourage businesses to use these methods to protect data, ultimately keeping local consumers’ data safer.

3. **Combine Data Elements (4) and (5):** We agree that the existing formulation in the state statute is confusing, but suggest combining the draft elements of (4) and (5), under the definition for “specified data element,” to further clarify that the risk of harm to an individual comes when a cybercriminal has access to both a financial or credit card account number and the password, not one or the other. The vast majority of states (46 out of 50) take an approach similar to the one we are proposing. In fact, these states generally combine the financial/credit card number with “any” security code or access code permitting access. To ensure that our amendments to the statute are not unintentionally read as unreasonably narrowing the language, we have added the “any” modifier to increase that alignment.

4. **Unauthorized Account Access:** No other state requires going through the formal notification process for a business where there are attempts to access a consumer’s online account. Instead, states have developed an approach to provide rapid notification in the manner in which the consumer interacts with business. Many of us commonly receive these emails encouraging us to change our passwords due to suspicious activity. While our offered amendments are tied to the confines of SB2292, we would be able to support an additional definition under “Personal Information,” as other states include, to read as follows:

“Personal information means **“either: (i) an individual’s first initial or first name, and last name, in combination with one more specified elements, when the personal information is not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable; or (ii) a username or email address, in combination with a password or security question and answer that would permit access to an online account.”** (Bold indicates our new proposed language).



# STATE PRIVACY & SECURITY COALITION

The notification method for the scenario in (ii) would also align with other states' provisions, allowing rapid notice for this type of breach and providing consumers with the tools to immediately protect themselves:

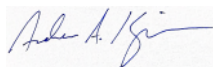
(4) In the case of a security breach involving personal information defined in paragraph (ii) of [the definition of personal information], and no other personal information defined in paragraph (i) of [definition of personal information], the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer.

In the case of a breach of the security of the system involving personal information defined in paragraph (ii) of [definition of personal information] for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

These provisions allow consumers to be rapidly notified when there is suspicious activity around account credentials, and to be notified in a secure manner; the effect of the second paragraph is to ensure that if, e.g., a consumer's email account has been hacked, the business does not send a password reset link to that email address.

We appreciate your consideration of these issues, and we would be happy to discuss any of the foregoing issues at your convenience.

Respectfully submitted,



Andrew A, Kingman  
General Counsel  
State Privacy & Security Coalition

---

---

# A BILL FOR AN ACT

RELATING TO PRIVACY.

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

1           SECTION 1. The legislature finds that House Concurrent  
2 Resolution No. 225, Senate Draft 1, Regular Session of 2019,  
3 convened the twenty-first century privacy law task force, whose  
4 membership consisted of individuals in government and the  
5 private sector having an interest or expertise in privacy law in  
6 the digital era. The concurrent resolution found that public  
7 use of the Internet and related technologies have significantly  
8 expanded in recent years and that a lack of meaningful  
9 government regulation has resulted in personal privacy being  
10 compromised. Accordingly, the legislature requested that the  
11 task force examine and make recommendations regarding existing  
12 privacy laws and rules to protect the privacy interests of the  
13 people of Hawaii.

14           The legislature finds that, following significant inquiry  
15 and discussion, the task force recommended that the outdated  
16 definition of "personal information" in chapter 487N, Hawaii  
17 Revised Statutes, which requires the public to be notified of

1111111

||| nMI ||| LE ||| |||

||||| | | | |



- 1        (1) An individual's social security number, either in its
- 2            entirety or more than the last four digits;
- 3        (2) Driver's license number, federal or state
- 4            identification card number, or passport number;
- 5        (3) A federal individual taxpayer identification number;
- 6        (4) An individual's financial account number or credit or
- 7            debit card number, in combination with
- 8            any security code, access code, personal identification
- 9            number, or password that would allow access to an
- 10           individual's account;
- 11        (6) Unique biometric data generated from a measurement or
- 12            analysis of human body characteristics used for
- 13            authentication purposes, such as a fingerprint, voice
- 14            print, retina or iris image, or other unique physical
- 15            or digital representation of biometric data;
- 16        (7) A private key that is unique to an individual and that
- 17            is used to authenticate or sign an electronic record;
- 18            and
- 19        (8) Health insurance policy number, subscriber
- 20            identification number, medical identification number,



1           or any other unique number used by a health insurer  
to  
2           identify a person.

3           "Specified data element" does not include medical  
4 information that is protected by the Health Insurance  
5 Portability and Accountability Act of 1996 and its enacting  
6 regulations or other applicable federal or state law."

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

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

13 ~~(1) Social security number;~~

14 ~~(2) Driver's licence number or Hawaii identification card~~  
15 ~~number; or~~

16 ~~(3)~~

17 ~~code, or password that would permit access to an~~

18 ~~individual's financial account.}~~

in combination with one or more specified data

20 elements, when the personal information is not encrypted,  
redacted, or otherwise protected by another method that renders the  
information unreadable or unusable. "Personal information" [does]  
shall not include

21 publicly available information that is lawfully made available

2022-1242 SB2292 SD1 SMA-1 doc





1 to the general public from federal, state, or local government  
2 records."

3 SECTION 3. Section 487N-2, Hawaii Revised Statutes, is  
4 amended by amending subsection (g) to read as follows:

5 "(g) The following businesses shall be deemed to be in  
6 compliance with this section:

- 7 (1) A financial institution that is subject to the federal  
8 Interagency Guidance on Response Programs for  
9 Unauthorized Access to Customer Information and  
10 Customer Notice published in the Federal Register on  
11 March 29, 2005, by the Board of Governors of the  
12 Federal Reserve System, the Federal Deposit Insurance  
13 Corporation, the Office of the Comptroller of the  
14 Currency, and the Office of Thrift Supervision, or  
15 subject to 12 C.F.R. Part 748, and any revisions,  
16 additions, or substitutions relating to the  
17 interagency guidance; [and]
- 18 (2) Any health plan or [healthcare] health care provider  
19 and its business associates that [E-s] are subject to  
20 and in compliance with the standards for privacy or  
21 individually identifiable health information and the



1 security standards for the protection of electronic  
2 health information of the Health Insurance Portability  
3 and Accountability Act of 1996[-7-]; and

4 (3) Any licensee that is subject to the Insurance Data  
5 Security Law pursuant to article 3B, chapter 431."

6 SECTION 4. This Act does not affect rights and duties that  
7 matured, penalties that were incurred, and proceedings that were  
8 begun before its effective date.

9 SECTION 5. Statutory material to be repealed is bracketed  
10 and stricken. New statutory material is underscored.

11 SECTION 6. This Act shall take effect upon its approval.

UJ1NM

VII i NH

ii 1

**Report Title:**

Privacy; Attorney General; Personal Information; Notice

**Description:**

Modernizes the definition of "personal information" for the purposes of notifying affected persons of data and security breaches. (SD1)

*The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.*

2022-1242 SB2292 SD1 SMA-1 doc



**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**

March 16, 2022

Rep. Gregg Takayama, Chair  
Rep. Linda Clark, Vice Chair  
and members of the House Committee on Higher Education & Technology  
Hawaii State Capitol  
Honolulu, Hawaii 96813

Re: **S.B. 2292, S.D. 1 (Privacy)**  
**Hearing Date/Time: Wednesday, March 16, 2022, 2:00 p.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 the following 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 (CPN) on January 28, 2022, the HFSA proposed an amendment to the definition of “specified data element” regarding social security numbers. The CPN Committee agreed and incorporated the HFSA’s proposed amendment in the Senate Draft 1 version which is before your Committee:

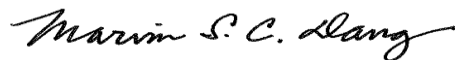
“Specified data element” means any of the following:

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

...

That wording in S.D. 1 should not be changed. As we explained in our CPN testimony, the usual practice in Hawaii (in the statutes, in the court rules, and for the financial industry) and in other states is to allow redacting, shortening, truncating, abbreviating, or limiting the display of an individual’s social security number down to the last 4 digits, i.e. xxx-xx-4321.<sup>1</sup> The S.D. 1 wording reflects that usual practice.

Thank you for considering our testimony.



MARVIN S.C. DANG  
Attorney for Hawaii Financial Services Association

(MSCD/hfsa)

---

<sup>1</sup> Various Hawaii statutes require or allow the public display or disclosure of the last 4 digits of a social security number (i.e. xxx-xx-4321) when a judgment is to be publicly recorded at the Bureau of Conveyances. See, e.g., HRS Secs. 501-151, 502-33, 504-1, and 636-3. Other Hawaii statutes require redacting or removing the first 5 digits of the social security number so that only the last 4 digits are displayed (i.e. xxx-xx-4321). See, e.g., HRS Secs. 15-4, 232-7, 232-18, 576D-10.5(f), and 803-6(b).



**Testimony of  
LISA McCABE  
CTIA**

**SB2292 SD1 Relating to Privacy. – OPPOSITION**

**House Committee on Higher Education & Technology**

**March 16, 2022**

Chair Takayama, Vice Chair Clark, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, thank you for the opportunity to provide this testimony in opposition to SB2292 SD1. As drafted, the bill contains overly broad definitions that would cause uncertainty regarding implementation and create confusion for both businesses and consumers.

Making the definitional changes to existing terms in the Hawaii statute as contemplated in SB2292 SD1, will have an impact on businesses operating in Hawaii and will cause complications with respect to compliance for businesses because it would create a data breach law in Hawaii that is not interoperable with other states. Regarding transactions on a national level, this legislation would inadvertently make Hawaii an outlier.

It is important to have a statute that is aligned with the other states, so that in the case of a data breach, notification to state residents is efficient and consistent. As contemplated in the bill, the information referenced in the definition of identifier, such as name, phone numbers, and email addresses, are widely available – even publicly available – and would dramatically increase the scope of what could constitute a data breach. The data elements covered in the bill are overly broad and cover a wide and vague range of “identifiers” combined with a single “specified data element.” This is a significant deviation from data breach laws in other states and would not provide additional security for Hawaii consumers in the event of a breach. However, it would place an additional compliance burden on businesses, as they would be required to segment data of Hawaii residents from other states causing additional inefficiencies.





We respectfully request that this measure be deferred until all the impacts of the bill are fully and completely identified and considered. Thank you for this opportunity to submit testimony.

March 15, 2022

The Honorable Gregg Takayama, Chair  
The Honorable Linda Clark, Vice Chair  
House Committee on Higher Education & Technology  
Conference Room 309

**Re: Senate Bill 2292, SD1 Relating to Privacy: Concerning the definition of Personal Information (Oppose)**

Dear Chair Takayama, Vice Chair Clark and Members of the Committee on Higher Education and Technology,

On behalf of RELX, a world-leading provider of technology solutions that support the government, insurance, and financial services industries in making communities safer, insurance rates more accurate, commerce more transparent, and processes more efficient, we respectfully request that you hold Senate Bill 2292, SD1 in your committee and not advance the measure this session while discussions with affected stakeholders can take place.

Currently, we have no issue with the state's existing data breach statute and would be supportive of an update. However, the changes suggested in the bill before you – especially with regard to the removal of the encryption and redaction language of the existing law – would have serious consequences for businesses and consumers alike. If this bill passes without amendment, breach notification would be triggered where there is no risk of harm to the consumer when the information is already encrypted and redacted. This would lead to consumers receiving countless meaningless notifications where no actual threat of identity theft exists.

If you feel it is absolutely necessary to move legislation on this issue, we ask that you adopt the language below with regard to the definitions which would accomplish the intent of the legislation by updating the statute to include specified data elements, while retaining the important encryption and redaction language from existing law.

**Suggested Definitions:**

*“Personal Information” means an individual’s first name or first initial and last name in combination with any one or more of the following specified data elements when either the name or the specified data element are not encrypted.*

*“Specified data element” means an individual’s social security number, either in its entirety or the last four or more digits; Driver’s license number, federal or state identification card number, or passport number; A federal individual taxpayer identification number; An individual’s financial account number or credit or debit card number in combination with the relevant security code, access code, personal identification number, or password that would allow access to an individual’s account; Protected health information as defined by the Federal Health Information Portability and Accountability Act; 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, digital representation of*

*biometric data; And a private key or other unique identifier used to authenticate or sign an electronic record.*

Thank you for your consideration of RELX concerns pertaining to Senate Bill 2292, SD1. We have an excellent track record of working with policymakers to craft meaningful privacy legislation. We would be pleased to offer the expertise of our privacy counsel should you have any questions regarding the language we have suggested or require additional materials. I can also be reached directly via e-mail at [london.biggs@relx.com](mailto:london.biggs@relx.com) or at 202-716-7867.

Sincerely,

*London Biggs*

London Biggs  
Director, State Government Affairs - West  
RELX Group



Testimony to the House Committee on Higher Education and Technology  
Wednesday, March 16, 2022  
2:00 pm

In opposition to SB 2292 SD1, Relating to Privacy

To: The Honorable Gregg Takayama, Chair  
The Honorable Linda Clark, 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 concerns:

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.



DATE: March 16, 2022

TO: Representative Gregg Takayama  
Chair, Committee on Higher Education and Technology

FROM: Mihoko Ito

RE: **S.B. 2292, S.D. 1 - Relating to Privacy**  
**Hearing Date: Thursday, March 16, 2022 at 2:00 p.m.**  
**Conference Room: 309**

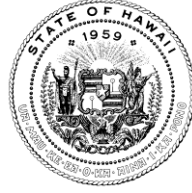
---

Dear Chair Takayama, Vice Chair Clark and Members of the Committee on Higher Education and Technology:

We offer this testimony on behalf of the Consumer Data Industry Association (CDIA). Founded in 1906, CDIA is the international trade association that represents more than 100 data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, fraud prevention, risk management, employment screening, tenant screening and collection services.

CDIA respectfully opposes SB 2292, SD1. This measure would significantly expand Hawaii's data breach law to cover a range of data identifiers which, in combination with "specified data elements" would trigger a required data breach notice to Hawaii consumers. This bill does not align with other state data breach laws, and it would be a significant cost for businesses to implement in order to comply. In addition, the combination of some of the identifiers and data elements do not pose a risk of harm that Hawaii consumer's identity would be compromised.

For the above reasons, CDIA opposes the bill and respectfully requests that the measure be held. Thank you for the opportunity to submit this testimony.



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  
House Committee Higher Education and Technology  
Wednesday, March 16, 2022  
2:00 p.m.  
State Capitol, Videoconference**

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

Chair Takayama 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.



March 16, 2022

The Honorable Gregg Takayama, Chair  
The Honorable Linda Clark, Vice Chair  
House Committee on Higher Education & Technology

**Senate Bill 2292 SD1 – Relating to Privacy**

Dear Chair Takayama, Vice Chair Clark, and Members of the Committee:

The Hawaii Association of Health Plans (HAHP) appreciates the opportunity to provide **comments** on SB 2292 SD1. HAHP is a statewide partnership of Hawaii’s health plans and affiliated organizations to improve the health of Hawaii’s communities together. The vast majority of Hawaii residents receive their health coverage through a health plan associated with one of our organizations.

HAHP believes that current Federal requirements under Health Insurance Portability and Accountability Act (HIPAA) provides significant health care consumer protection and HIPAA has its own enforcement mechanism and penalties for health care entities. As such, HAHP suggests the following edit (changes in red) to pages 5-6 of the bill to prevent any potential inadvertent conflict between Hawaii law and Federal requirements and enforcement of HIPAA:

“(2) Any health plan or [~~healthcare~~] health care provider and ~~its~~ their business associates that [~~is~~] are subject to ~~and in compliance with~~ the standards for privacy ~~or of~~ individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996.”

Thank you for allowing us to submit our comments on SB 2292 SD1.

Sincerely,

HAHP Public Policy Committee

cc: HAHP Board Members

[hahp.org](http://hahp.org) | 818 Keeaumoku St., Honolulu, HI 96814 | [info@hahp.org](mailto:info@hahp.org)

AlohaCare | HMAA | HMSA | Humana | HWMG | Kaiser Permanente | MDX Hawaii | Ohana Health Plan | UHA Health Insurance | UnitedHealthcare

March 14, 2022

S.B. 2292 Relating to Privacy

House Committee on Education and Technology

Hearing Location: Hawaii State Capitol, 415 South Beretania Street, Conference Room 309

Hearing Date/Time: Wednesday, March 16, 2022, 2:00 PM

Dear Chair Takayama, Vice Chair Clark, 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 people 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 four digits of the SSN, then all that protects a local's SSN is the middle two digits. In some years, as few as nineteen combinations were used for these two middle digits; and these combinations are publically available. The situation is even worse for adolescents raised in Hawaii. For SSNs issued between 2004 and 2011, the first three digits are either 750 or 751 and only eleven middle digits were used.

In summary, for anyone who received their SSN in Hawaii before 2011, a breach of four digits leaves only the two non-random middle digits to protect a person's SSN. Please restore this aspect of the bill to the original version and protect people who were raised in Hawaii.

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

*Kelly McCanlies*

Kelly McCanlies

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



Presentation to The  
Committee on Higher Education & Technology  
Wednesday, March 16, 2022, 2:00 P.M.  
State Capitol Conference Room 309 & Videoconference

**Testimony on SB 2292, SD1 With Proposed Amendments**

TO: The Honorable Gregg Takayama, Chair  
The Honorable Linda Clark, 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.

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 lead 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, lines 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 page 4, lines 20-21, 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, SD1. Please let us know if we can provide further information.

Neal K. Okabayashi  
(808) 524-5161