



STATE OF HAWAII | KA MOKU'ĀINA 'O HAWAI'I
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS
KA 'OIHANA PILI KĀLEPA
335 MERCHANT STREET, ROOM 310
P.O. BOX 541
HONOLULU, HAWAII 96809
Phone Number: (808) 586-2850
Fax Number: (808) 586-2856
cca.hawaii.gov

JOSH GREEN, M.D.
GOVERNOR | KE KIA'ĀINA

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

NADINE Y. ANDO
DIRECTOR | KA LUNA HO'OKELE

DEAN I HAZAMA
DEPUTY DIRECTOR | KA HOPE LUNA HO'OKELE

Testimony of the Department of Commerce and Consumer Affairs

**Before the
House Committee on Consumer Protection and Commerce
Wednesday, March 13, 2024
2:05 p.m.
State Capitol, Conference Room 329 and via Videoconference**

**On the following measure:
S.B. 2695, S.D. 1, RELATING TO PRIVACY**

Chair Nakashima and Members of the Committee:

My name is Gordon Ito, and I am the Insurance Commissioner of the Department of Commerce and Consumer Affairs' (Department) Insurance Division. The Department offers comments on this bill.

The purpose of this bill is to add definitions of "identifier" and "specified data element" and amends the definition of "personal information" for the purposes of notifying affected persons of data and security breaches under existing state law that governs the security breach of personal information; include licensees subject to the Insurance Data Security Law, article 3B, chapter 431, Hawai'i Revised Statutes, among the businesses deemed compliant with security breach notice requirements under existing state law.

We have concerns with the new paragraph (3) referencing HRS section 431, article 3B at page 4, lines 4 to 5 of this bill and respectfully suggest that this language be removed to avoid confusion and statutory interpretation issues. With respect to

consumer notices, the Insurance Data Security Law requires that notices be provided in accordance with chapter 487, but does not set forth separate provisions for consumer notification. See HRS § 431:3B-303. The proposed new paragraph (3) in this bill does not appear to account for this, and instead appears to erroneously presume that the Insurance Data Security Law includes its own process for consumer notifications. As such, the proposed new paragraph (3) would likely create statutory interpretation issues and even be used to argue that insurers are not required to issue consumer notices.

Thank you for the opportunity to testify.



STATE OF HAWAII | KA MOKU'ĀINA 'O HAWAI'I
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS
KA 'OIHANA PILI KĀLEPA
335 MERCHANT STREET, ROOM 310
P.O. BOX 541
HONOLULU, HAWAII 96809
Phone Number: (808) 586-2850
Fax Number: (808) 586-2856
cca.hawaii.gov

JOSH GREEN, M.D.
GOVERNOR | KE KIA'ĀINA

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

NADINE Y. ANDO
DIRECTOR | KA LUNA HO'OKELE

DEAN I HAZAMA
DEPUTY DIRECTOR | KA HOPE LUNA HO'OKELE

Testimony of the Department of Commerce and Consumer Affairs

Office of Consumer Protection

Before the
House Committee on Consumer Protection & Commerce
Wednesday, March 13, 2024
2:05 PM
Via Videoconference
Conference Room 329

On the following measure:
S.B. 2695, S.D. 1, RELATING TO PRIVACY

Chair Nakashima and Members of the Committee:

My name is Mana Moriarty, 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 to update Hawaii's data security law, Hawaii Revised Statutes Chapter 487N, our state's first line of defense against unlawful access to and acquisition of protected information. OCP defers to the Department's Insurance Division in regard to Section 3 of this bill.

In 2006, Hawaii was one of the first states to enact a data security law. Since 2006, technology has evolved rapidly and bad actors exploit vulnerabilities in computer databases with increased frequency—e.g., the recent HMSA and Change Healthcare data breaches—but our data security law has not been amended to meet these developments.

Businesses that collect or store data digitally have a responsibility to protect personal information from unlawful access and acquisition. HRS chapter 487N sets forth when a business or government agency must notify (i) a consumer that their personal information has been breached, and (ii) other government agencies, such as OCP.

S.B. 2695, S.D. 1 expands 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. As noted in other supportive testimony, the law must evolve to recognize that names and initials are no longer our only identifiers; social media profiles, emails, and phone numbers, can be equally indicative of our identities. The HMSA data breach which affected more than 735,000 Hawaii residents divulged medical account numbers, a category of information not currently recognized in HRS chapter 487N as personal information. Expanding the definition of “personal information” will enhance consumer protections involving privacy and align Hawaii more closely with the 31 states that have a more expansive definition of personal information in their data breach law.

Those professing concern that this bill fails to recognize the value of encryption should read more closely. This bill changes the definition of personal information, but the definition of security breach in HRS chapter 487N is unchanged; a security breach “means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur and that creates a risk of harm to a person.”

For the same reason, those professing concern that the bill creates unintended consequences by making run-of-the mill court filings into security breaches may wish to re-read the definition of personal information. “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

OCP supports this bill, with the amendments offered by Insurance Division as to Section 3. Thank you for the opportunity to testify on this bill.



STATE OF HAWAII
DEPARTMENT OF EDUCATION
KA 'OIHANA HO'ONA'AUAO
P.O. BOX 2360
HONOLULU, HAWAII 96804

Date: 03/13/2024

Time: 02:05 PM

Location: 329 VIA VIDEOCONFERENCE

Committee: House Consumer Protection &
Commerce

Department: Education

Person Testifying: Keith T. Hayashi, Superintendent of Education

Title of Bill: SB 2695, SD1 RELATING TO PRIVACY.

Purpose of Bill: Adds definitions of "identifier" and "specified data element" and amends the definition of "personal information" for the purposes of notifying affected persons of data and security breaches under existing state law that governs the security breach of personal information. Includes licensees subject to the Insurance Data Security Law, article 3B, chapter 431, Hawaii Revised Statutes, among the businesses deemed compliant with security breach notice requirements under existing state law. Takes effect 7/1/2040. (SD1)

Department's Position:

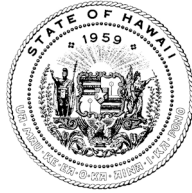
The Hawaii State Department of Education (Department) supports SB 2695 SD 1's addition of identifiers and data elements to the Hawaii Revised Statutes (HRS) Chapter 487N, as the current definition is outdated.

Hawaii's security breach notification laws were enacted in 2006 and codified in HRS Chapter 487N, yet advancements in technology have made identity theft far easier than when the law was enacted. Expanding the definitions will provide increased security to protect our student and staff information especially when working with vendors who provide services to the Department.

SB 2695 SD 1 corrects existing statutory inadequacies by adding in the additional Identifiers and specified data elements enhancing data security for everyone.

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

JOSH GREEN, M.D.
GOVERNOR
KE KIA'AINA



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

Written Testimony of
DOUGLAS MURDOCK
Chief Information Officer
Enterprise Technology Services

Before the
HOUSE COMMITTEE ON CONSUMER PROTECTION AND COMMERCE
WEDNESDAY, MARCH 13, 2024

SENATE BILL 2695 SD1
RELATING TO PRIVACY

Dear Chair Nakashima, Vice Chair Sayama, 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.



ABC Stores
766 Pohukaina Street
Honolulu, Hawaii 96813-5391
www.abcstores.com

Telephone: (808) 591-2550
Fax: (808) 591-2039
E-mail: mail@abcstores.com

To: Committee on Consumer Protection & Commerce

Re: SB 2695 SD1 Relating to Privacy

Date: March 13, 2024

Time: 2:05 p.m.

Place: Conference Room 329

Position: Oppose bill as drafted

Good afternoon, Chairperson Mark M. Nakashima, Vice Chair Jackson D. Sayama and members of the Committee on Consumer Protection & Commerce. I am Curtis Higashiyama Employee Relations and Government Affairs Manager, and we appreciate this opportunity to testify.

ABC Stores **Opposes as drafted** bill SB2695 SD1. Adds definitions of "identifier" and "specified data element" and amends the definition of "personal information" for the purposes of notifying affected persons of data and security breaches under existing state law that governs the security breach of personal information. Includes licensees subject to the Insurance Data Security Law, article 3B, chapter 431, Hawaii Revised Statutes, among the businesses deemed compliant with security breach notice requirements under existing state law. Takes effect 7/1/2040. (SD1)

While we appreciate the intent of the bill to prevent risk of identity theft, consumer fraud and improved notification to consumers from businesses, we ask the committee to review what is labeled as "identifiers" and "specific data elements," as these would trigger a security breach by definition. As written, it appears too broad and will benefit everyone to have a narrower scope for both "identifier" and "Specific Data" elements.

As an example: "Specific data element:" An individual's social security number, either in its entirety or the last four or more digits. Many businesses keep redacted credit card records on file (last 4 digits) to meet record keeping and processing requirements.

We urge you to hold this measure as drafted. Thank you for the opportunity to testify.

Mahalo,
Curtis Higashiyama
ABC Stores
Employee Relations and Government Affairs



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Southwest | Telephone 505.402.5738
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetSW

March 12, 2024

Representative Mark Nakashima
Chair, Consumer Protection and Commerce Committee
Hawaii State Capitol
415 South Beretania Street, Room 432
Honolulu, HI 96813

Representative Jackson Sayama
Vice Chair, Consumer Protection and Commerce Committee
Hawaii State Capitol
415 South Beretania Street, Room 406
Honolulu, HI 96813

Re: SB 2695 (Lee) – Data Breach Notifications– OPPOSE

Dear Chair Nakashima, Vice Chair Sayama and Members of the Committee,

TechNet must respectfully oppose SB 2695 (Lee), a bill that attempts to modernize the state's data breach notification requirements but that may have some unintended consequences. Recent amendments have not resolved our concerns.

TechNet is the national, bipartisan network of technology companies that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over five million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

Our member companies place a high priority on consumer privacy. The technology industry is fully committed to securing privacy and security for consumers and engages in a wide range of practices to provide consumers with notice, choices about how their data are used, and control over their data.

We believe this bill is well intentioned, however, the current definitions are overbroad and could lead to confusing notices for consumers in instances when their data isn't at risk. For example, information that is encrypted or otherwise protected presents no risk to consumers if the hacker does not also have the encryption key. Requiring consumers to be notified if this type of information is accessed in a breach would be potentially misleading. Furthermore, this bill's definitions even conflict with other bills the legislature is considering, such as SB 974 (Lee), which would establish a comprehensive data privacy act for Hawai'i.

We suggest aligning the definitions and standards in this bill to ensure interoperability with other states. This alignment will ensure consumers receive consistent and efficient notices across state lines, without the need to separate out Hawaiian residents for a distinct notice.

Thank you for your consideration. If you have any questions regarding TechNet's position on this bill, please contact Dylan Hoffman, Executive Director, at dhoffman@technet.org or 505-402-5738.

Sincerely,

A handwritten signature in black ink, appearing to be 'DH', written over a horizontal line.

Dylan Hoffman
Executive Director for California and the Southwest
TechNet



**TESTIMONY OF TINA YAMAKI, PRESIDENT
RETAIL MERCHANTS OF HAWAII
MARCH 13, 2023
Re: SB 2695 SD1 RELATING TO PRIVACY.**

Good afternoon, Chair Nakashima members of the House Committee on Consumer Protection and Commerce. I am Tina Yamaki, President of the Retail Merchants of Hawaii and I appreciate this opportunity to testify.

The Retail Merchants of Hawaii was founded in 1901 and is a statewide, not for profit trade organization committed to supporting the growth and development of the retail industry in Hawaii. Our membership includes small mom & pop stores, large box stores, resellers, luxury retail, department stores, shopping malls, on-line sellers, local, national, and international retailers, chains, and everyone in between.

While we understand the intent of this bill, we respectfully oppose SB 2695 SD1. This measure adds definitions of "identifier" and "specified data element" and amends the definition of "personal information" for the purposes of notifying affected persons of data and security breaches under existing state law that governs the security breach of personal information. Includes licensees subject to the Insurance Data Security Law, article 3B, chapter 431, Hawai'i Revised Statutes, among the businesses deemed compliant with security breach notice requirements under existing state law; and takes effect 7/1/2040.

We agree that with the rapid pace of technological evolution, we must remain vigilant. However, the definitions in this measure are far too broad and have unintended consequences for businesses. In the cases of customers' information that was NOT at risk, but is sent a notification, the customer may be confused as to if there was a breach or not or misleading that their information is at risk when it is not.

We would also like to point out that Email addresses are commonly used throughout a businesses' ecosystem and they have not been treated as an identifier requiring special protection. However, when an email address is used as a username to access an online account or profile that's already covered under "a user name for an online account".

Hawaii's definitions should be more in line with the other 49 states especially for data breach notifications.

Mahalo again for this opportunity to testify.

TO: Chair Nakashima, Vice Chair Sayama
House Committee on Consumer Protection & Commerce

SUBJECT: Testimony on SB2695, Relating to Privacy

DATE: Wednesday, March 13, 2024

TIME: 2:05 PM

LOCATION: Conference Room 329 & Videoconference

Dear Chair Nakashima, Vice Chair Sayama, and members of the committee:

Thank you for the opportunity to testify. As the youth advocacy collective Student Advocates for Responsible Technology (START), we stand in **support** of SB2695. In its current form, HRS 487N falls drastically short of addressing all forms of data breaches. Growing up with the internet, we know that our names and initials are no longer our only “identifiers,” with social media profiles, emails, and phone numbers being equally indicative of our identities.

We also believe in SB2695 because it amends the definition of “personal information” to account for biometrics. Whether it be through products like Amazon’s Alexa or the recognition systems recently installed at Daniel K. Inouye International Airport, we share biometric data every day, making the need for a reformed privacy law all the more imperative.

Last month, a cyberattack staged against the Hawaii Medical Service Association (HMSA) divulged over four-hundred thousand members’ medical data, including account numbers, a category of information not covered by HRS 487N. With families affected by the cyberattack, we believe all the more strongly that SB2695 needs to be passed in order to protect others from data breaches.

Thank you for the opportunity to submit testimony. We continue to pledge our **strong support** for SB2695.

Reina Gammarino
Student Advocates for Responsible Technology (START)
starthi.org

STATE PRIVACY & SECURITY COALITION

March 12, 2024

Chair Mark M. Nakashima
Vice Chair Jackson D. Sayama
Committee on Consumer Protection and Commerce
Hawaii House of Representatives
415 South Beretania Street
Honolulu, HI 96813

Re: SB 2695 – Oppose Unless Amended

Dear Chair Nakashima, Vice Chair Sayama, and Members of the Committee,

The State Privacy & Security Coalition, a coalition of over 30 companies and six trade associations in the retail, payment card, automotive, healthcare, technology, and telecom sectors (nearly all of whom serve consumers in the state of Hawaii) respectfully opposes SB 2695 unless amended. We would very much 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, 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.

Our suggested amendments 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 these 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 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

STATE PRIVACY & SECURITY COALITION

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:** Under current Hawaii law, the value of encrypted data is recognized. This is because 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 for multiple reasons. 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, including a safe harbor for unusable encrypted data will further encourage businesses to use these methods to protect data, ultimately keeping local consumers’ data safer from cybercriminals.

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 a similar approach 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.

Accordingly, we recommend that (4) and (5) be combined into one subsection to read as follows: “An individual’s financial account number, or credit card or debit card number in combination with a security code, access code, personal identification number, or password that would allow access to an individual’s account.”

4. **Amend the “personal information” definition:** Hawaii would be an outlier from all other states by requiring a 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 SB 2695, 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**

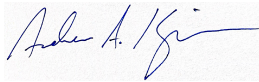
STATE PRIVACY & SECURITY COALITION

password or security question and answer that would permit access to an online account. (Bold indicates our new proposed language).

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
Counsel, State Privacy & Security Coalition



**Testimony of
JAKE LESTOCK
CTIA**

In Opposition to Hawaii Senate Bill 2695

**Before the
House Committee on Consumer Protection & Commerce**

March 13, 2024

Chair Nakashima, Vice Chair Sayama, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I submit this testimony in opposition to Senate Bill 2695. As currently drafted, the bill contains overly broad definitions that would cause uncertainty regarding implementation and create confusion for both businesses and consumers.

Implementing the proposed definitional changes outlined in SB 2695 will have a significant impact on businesses operating in Hawaii. The changes proposed would introduce complexities in compliance as it establishes a unique data breach law for Hawaii that is incompatible with those of other states. This lack of interoperability would isolate Hawaii and create problems for businesses and confusion for Hawaiians. It is vital 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 recommend harmonizing the definitions and standards in this bill to ensure compatibility with those of other states. We respectfully oppose this legislation as currently drafted and request that the bill not move forward in its current form. Thank you for the opportunity to submit this testimony and for your consideration.



Testimony to the House Committee on Commerce & Consumer Protection
Wednesday, March 13, 2024
Conference Room 329

Comments Re: SB 2695 - Relating to Privacy

To: The Honorable Mark Nakashima, Chair
The Honorable Jackson Sayama, 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 47 Hawaii credit unions, representing over 864,000 credit union members across the state.

HCUL offers the following comments regarding SB 2695, Relating to Privacy. This bill would add definitions of "identifier" and "specified data element" and amends the definition of "personal information" for the purposes of notifying affected persons of data and security breaches, and includes licensees subject to the Insurance Data Security Law, article 3B, chapter 431, Hawai'i Revised Statutes, among the businesses deemed compliant with the chapter's security breach notice requirements.

While we understand the intent of this bill, we have some 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. We also concur with the testimony presented by the Hawaii Bankers Association.

While we understand the need for data privacy legislation, we would prefer a more comprehensive approach to this issue, to avoid possible unintended consequences for our members.

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



SanHi

GOVERNMENT STRATEGIES

A LIMITED LIABILITY LAW PARTNERSHIP

DATE: March 13, 2024

TO: Representative Mark M. Nakashima
Chair, Committee on Consumer Protection & Commerce

FROM: Mihoko Ito

RE: **S.B. 2695, S.D. 1 - Relating to Privacy**
Hearing Date: Wednesday, March 13, 2024 at 2:05 p.m.
Conference Room: 329

Dear Chair Nakashima, Vice Chair Sayama, and Members of the Committee on Consumer Protection & Commerce:

We offer this testimony on behalf of the Consumer Data Industry Association (CDIA). The Consumer Data Industry Association (CDIA) is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check companies, and others.

CDIA **opposes** S.B. 2695, S.D. 1, which amends Hawaii's security breach law by adding definitions of "identifier" and "specified data element" and amends the definition of "personal information" for the purposes of notifying affected persons of data and security breaches.

CDIA appreciates the legislature's intent to update Hawaii's current data breach statute. However, CDIA believes that the changes being proposed are overbroad and do not reflect data elements that truly present a risk of identity theft or other types of consumer fraud to 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.

Perhaps most concerning is that, unlike every other state which excludes from a security breach encrypted or otherwise protected information, this legislation deviates from this practice and would create a data breach law for Hawaii that is not interoperable with other states and would inadvertently make the state an outlier. The removal of the encryption and redaction language of the existing law as proposed by SB 2695, S.D.1 would have serious unintended consequences for businesses and consumers alike.

Consumer reporting agencies are already highly regulated and required to safeguard sensitive data and financial information via multiple federal statutes.

We oppose this measure as currently drafted and request that the bill not move forward in its current form.

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



SanHi

GOVERNMENT STRATEGIES

A LIMITED LIABILITY LAW PARTNERSHIP

DATE: March 13, 2024

TO: Representative Mark Nakashima
Chair, Committee on Consumer Protection and Commerce

FROM: Mihoko Ito / Tiffany Yajima

RE: **S.B. 2695 S.D.1 - Relating to Privacy**
Hearing Date: Wednesday, March 13, 2024 at 2:05 p.m.
Conference Room 329 & Videoconference

Dear Chair Nakashima, Vice Chair Sayama and Members of the Committee on Consumer Protection & Commerce:

We submit this testimony on behalf of the Hawaii Bankers Association (HBA). HBA represents seven Hawai'i banks and one bank from the continent with branches in Hawai'i.

HBA submits **comments** regarding S.B. 2695, S.D.1, which amends the definition of "personal information." While we do not object to the substance of the bill, we believe that the bill can be improved by including the amendments we are proposing in this testimony.

We believe that the definition of "Identifier" in its current form is vague as to some elements. Because these identifiers combined with a data element would trigger business obligations if a security breach occurs, we believe the bill should be as specific as possible in defining the identifiers that would trigger a security breach.

1) We would recommend amending the name identifier at page 2, line 19. Using a name by first name or initial as an identifier as the bill currently reads can be problematic, because there are many combinations of names, initials, and last names that people may use when interfacing with businesses. We think more clarity is provided with the following language:

"A name used by an individual, including the combination of the first name, any initials in the name whether at the beginning or middle of the name, or a nickname combined with the last name."

2) We also recommend an amendment to the inclusion of financial account numbers and debit or credit card numbers at page 3, lines 8 and 9. Redacted card numbers are common in data that might be kept in business files, like in credit card receipt records. The risk of harm occurs with these numbers where the entirety of a financial account number or credit/debit card number is released. We would propose to amend this language to read:

“An individual’s financial account number or credit or debit card number unless redacted.”

3) We would also recommend that the exclusion for public information should not be limited to federal, state or local government records. There is no reason that the exception for publicly available information should be restricted to information made available by the government, since that same information could be published by the media, blog, disseminated on television, radio or podcast or otherwise. In some cases, it would be difficult for businesses to ascertain whether information it retained was made available from federal, state, or local government records. We would therefore suggest that this public information exclusion can be improved by deleting “from federal, state, or local government records”, at page 5, lines 2-5 as follows:

“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.

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

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 13, 2024

Rep. Mark M. Nakashima, Chair
Rep. Jackson D. Sayama, Vice Chair
and members of the House Committee on Consumer Protection & Commerce
Hawaii State Capitol
Honolulu, Hawaii 96813

Re: **S.B. 2695, S.D. 1 (Privacy)**
Hearing Date/Time: Wednesday, March 13, 2024, 2:05 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 opposes the bill as drafted.

This Bill does the following: (a) adds definitions of "identifier" and "specified data element" and amends the definition of "personal information" for the purposes of notifying affected persons of data and security breaches under existing state law that governs the security breach of personal information; and (b) includes licensees subject to the Insurance Data Security Law, article 3B, chapter 431, Hawai‘i Revised Statutes, among the businesses deemed compliant with security breach notice requirements under existing state law.

In this Bill, “personal information”, for the purpose of a security breach of personal information, means an “identifier” in combination with one or more “specified data elements.” (See page 5, lines 7 through 18.)

On page 3, line 1 through page 4, line 2 of this Bill the following definition of “specified data element” is added:

“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;

. . .

(bold and yellow highlight added.)

Paragraph 1 of the definition of “specified data element” relates to an individual’s social security number. We agree with intent of the wording in the first phrase of paragraph 1 which includes an individual’s social security number “**in its entirety**” (i.e. the entire 9 digits such as **987-65-4321**) as a specified data element. This is similar to the intent of the wording in the other paragraphs of the “specified data element” definition, e.g., a “driver’s license number” (see paragraph 2), a “federal individual taxpayer identification number” (see paragraph 3), an “individual’s financial account number” (see paragraph 4), etc.

That’s also consistent with existing Hawaii statutes which prohibit communicating or making publicly available a person’s entire social security number, i.e. all 9 digits are protected from being displayed.¹

However, we disagree with the wording in the second phrase of paragraph 1 in the definition of “specified data element” which includes “the last four or more digits” of an individual’s social security number. As the second phrase is written, a “specified data element” would be when the last 4 or more digits is displayed, including the following: **xxx-xx-4321**.

That second phrase is problematic. The usual practice in Hawaii (in the Hawaii Revised 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-4321.² Because of existing laws and practices, a display of the last 4 digits should NOT be a “specified data element” for the purpose of a security breach under this Bill.

We wouldn’t object if paragraph 1 is reworded to include as a “specified data element” **more than** the last 4 digits of a social security number. For example, displaying xxx-x**5-4321** should be a “specified data element.”

Accordingly, we offer two versions of a proposed amendment to this Bill. Under our proposed version #1 below, we recommend that only when the entire 9 digits of the social security number is displayed, that would be a “specified data element.” This would be consistent with the other paragraphs in the definition of “specified data element.”

Under our proposed version #2 below, we recommend that, separate from displaying the entire 9 digits of the social security number, when **more than** the last 4 digits is shown, that would be a “specified data element” for the purpose of a security breach of personal information. Displaying “more than” xxx-xx-4321 would be a “specified data element.” Thus, displaying xxx-x**5-4321** should be ... and would be ... a “specified data element.” But displaying xxx-xx-**4321** should **NOT** be ... and would **NOT** be ... a “specified data element.”

BELOW ARE TWO ALTERNATE PROPOSED VERSIONS:

¹ See Hawaii Revised Statutes Sec. 487J-2(a)(1) relating to social security number protection. See also the definition of “confidential personal information” in HRS Sec. 708-800.

² Among the Hawaii statutes which require or allow the public display or disclosure of the last 4 digits to be displayed (i.e. xxx-xx-4321) are those where the last 4 digits of an individual’s social security number are displayed when a judgment is to be publicly recorded at the Bureau of Conveyances. See, for example, HRS Secs. 501-151, 502-33, 504-1, and 636-3. Other Hawaii statutes which require redacting or removing the first 5 digits of the social security number so that only the last 4 digits are displayed include HRS Secs. 15-4, 232-7, 232-18, 576D-10.5(f), and 803-6(b).

PROPOSED AMENDMENT - VERSION #1:

“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;

...

OR

PROPOSED AMENDMENT - VERSION #2:

“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 [or more] digits;

...

Thank you for considering our testimony.



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



March 11, 2024

Representative Mark M. Nakashima
Chair, Committee on Consumer Protection & Commerce

Re: S.B. 2695 S.D. 1: Revised definition of Personal Information (Oppose unless Amended)

Dear Chair Nakashima, Vice Chair Sayama, and members of the Committee,

On behalf of RELX, a world-leading provider of technology solutions that support the government, insurance, and financial services industries, we respectfully **oppose** advancement of S.B. 2695 S.D. 1 unless amended to restore the removal of encryption language currently included in the existing law.

Removing the encryption language from existing law as the bill proposes in the new definition of personal information would have serious consequences for businesses and consumers alike. If this bill passes unamended, breach notification would be triggered when the information is already encrypted and there is no risk of harm to the consumer. Without this amendment, consumers will receive countless meaningless notifications where no actual threat of identity theft exists.

We ask that you restore the encryption language in current law as provided below without other changes to the bill which would accomplish the intent of the legislation by updating the statute to include specified data elements, while retaining the important encryption language currently relied upon by businesses.

Specifically, we ask the committee to amend S.B. 2695 S.D. 1 on page 4, line 7 to read as follows:

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, when either the identifier or specified data elements are not encrypted. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."



Thank you for your consideration of RELX concerns pertaining to S.B. 2695 S.D. 1. 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 or at 202-716-7867.

Sincerely,

London Biggs

London Biggs
Director, State Government Affairs - West
RELX



To: Hawai'i State House Committee on Consumer Protection & Commerce
Hearing Date/Time: Wednesday, March 13, 2024 at 2:05 PM
Place: Hawai'i State Capitol, Rm. 325 and videoconference
Re: Testimony of Planned Parenthood Alliance Advocates – Hawai'i in strong support of SB 2695

Chair Nakashima and members of the Committees,

Planned Parenthood Alliance Advocates strongly supports SB 2695. Hawai'i must take steps to protect people from data breaches and bolster data privacy as part of its efforts to support access to all critical health care.

SB 2695 would notify consumers when their data is not kept private, an important step towards protecting their rights, particularly in the context of health care. Stigma, fear of prosecution, and harassment from anti-abortion and anti-LGBTQ groups are significant barriers to accessing reproductive and gender affirming health care, and PPAA believes that everyone should be able to access the health care they need without their personal health information being shared without their permission or knowledge.

We are grateful that the House already passed HB 1566. This bill would require Hawai'i entities to disclose how patient information may be used and disallow collecting, sharing, or selling health data without consumer consent. All people deserve to be informed and given the opportunity to consent to the collection and distribution of their personal, private health information, and we encourage lawmakers to pass SB 2695 in tandem with HB 1566 to comprehensively support protecting health information.

Planned Parenthood understands firsthand how data in the wrong hands can lead to violence and harassment of patients and providers. Right now, much health and patient data is easily accessible and dangerous. In May 2022, SafeGraph, a location data broker, sold the aggregated location data of people who visited abortion clinics, including more than 600 Planned Parenthoods over a one week period for just \$160. The data showed where patients traveled from, how much time they spent at the health centers, and where they went afterwards. Those who obtain healthcare, including abortions or gender affirming care, should not be subjected to targeted ads about their private health care decisions, and people should not have their locations tracked and shared via geotargeting when seeking health care. Similarly, data breaches revealing similar information could be used to target and harass patients and providers, and consumers deserve to know when this information has been breached.

SB 2695 is especially important in protecting already-vulnerable populations like domestic violence survivors, communities of color, the LGBTQ+ community, undocumented immigrants, young people, and people with disabilities. These communities are at an increased risk of surveillance and criminalization and face heightened danger when their health data is leaked and shared by harmful actors.

Patients' data should not be left vulnerable to be shared by anti-abortion and anti-LGBTQ groups, used in out-of-state prosecutions, or employed for targeted advertising when it is breached. Thank you for your support of SB 2695 to keep patients and providers safe from harassment, violence, and prosecutions.

March 12, 2024

SB 2695 SD1 Relating to Privacy
House Committee on Consumer Protection and Commerce
Hearing Date/Time: Wednesday, March 13, 2024, 2:05 PM
Place: Conference Room 329, State Capitol, 415 South Beretania Street

Dear Chair Nakashima, Vice Chair Sayama, and members of the Committee:

I write in SUPPORT of SB 2695. As a privacy expert, I have worked in data privacy for almost 20 years and served on the 21st Century Privacy Law Task Force created by the Legislature.

History:

In 2006, Hawaii was one of the first states to pass a data breach notification law (487-N). By 2018, all 50 states had similar laws. Without them, most companies have no obligation to tell consumers when their data is hacked, and we would not learn of major data breaches like Target and Equifax, which affected over 180 million consumers collectively.

In the last 15 years, the amount of personal information collected about Americans has grown exponentially. In response, most states have updated their data breach notification law and passed additional privacy legislation; 31 states now have more data elements identified in their laws than Hawaii. Hawaii should remain mainstream by updating our privacy law, too.

Current Issues This Bill Solves:

Identifiers: One example of why this update is needed is because our state data breach notification law (HRS 487-N) requires a person's name to be compromised, along with sensitive data, in order for a breach to have occurred.

To use Chair Nakashima as an example, the loss of his name (Mark Nakashima) plus his SSN is a breach, but the loss of his email address (repnakashima@capitol.hawaii.gov) and his SSN is not. Since his name and email address are closely aligned AND publically available on the state legislature's website, the risk of identity theft is the same in either case, but they are treated completely differently under the current law.

Last 4 of Social: Another example is the idea of protecting the last 4 digits of an SSN vs. the whole SSN. Every person born in Hawaii before 2004 has an SSN that starts with 575 or 576. So the common question "where did you go to high school?" is tantamount to asking "what the first 3 digits of your SSN?"

For most people in Hawaii, if the last 4 digits are breached, all that protects their SSN is the middle 2 digits. Moreover, in some years, as few as 9 sets of middle digits were used. So if the last 4 digits are breached, it is extremely easy to reverse engineer the whole SSN.

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

Kelly McCanlies

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

