LATE LATE

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

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

STATE OF HAWAII | KA MOKUʻĀINA ʻO HAWAIʻI
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS
KA ʻOIHANA 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

NADINE Y. ANDO
DIRECTOR | KA LUNA HOʻOKELE

DEAN I HAZAMA
DEPUTY DIRECTOR | KA HOPE LUNA HOʻOKELE

Testimony of the Department of Commerce and Consumer Affairs

Office of Consumer Protection

Before the
Senate Committee on Commerce and Consumer Protection
Wednesday, February 19, 2025
9:30 a.m.
Via Videoconference
Conference Room 229

On the following measure:
S.B. 1038 RELATING TO PRIVACY

Chair Keohokalole 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 appreciates the intent and offers comments on this bill.

The purpose of this bill is to implement the recommendation of the twenty-first century privacy law task force by expanding the scope of the state data breach notification law, HRS Chapter 487N. Among other things, this bill takes the protective approach of requiring a business to notify an individual when an unknown actor obtains unauthorized access to the individual's email address in combination with:

A password which would allow access to the email account;

Unique biometric data; or

Health insurance policy number, subscriber identification number, medical identification number, or any other unique number used by a health insurer to identify a person.

The existing state data breach notification law, HRS 487N-2, requires businesses to provide notification of a security breach to an individual who is the owner of the information subjected to the security breach. Appropriate guardrails are already in place to ensure that the reporting statute does not require reports in instances of unauthorized access that do not create a risk of harm to a person.

S.B. 1038 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. This will enhance consumer protections involving privacy and align with legislation enacted in other jurisdictions. Dozens of jurisdictions require data breach notification in response to instances of security breaches involving email accounts and passwords that allow access to the email account. A comprehensive list can be compiled for the Committee. Defining personal information to include email addresses is consistent with how personal information is defined in Hawaii's criminal statutes. HRS section 708-800 includes as "personal information" "an electronic mail address ... a password used for accessing information, ... alone or in conjunction with other information, to confirm the identity of an actual or fictitious person."

Generally, the Department supports S.B. 1038's expansion of the definition "personal information" in Hawaii Revised Statutes (HRS) chapter 487N, with the Department's recommended amendments. 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 easily accessible to criminals who engage in identity theft. Hawaii is far from unique in this regard. As of 2025, all 50 states have data breach notification laws that prescribe when consumers must be notified when their "personal information" has been breached.

Recommended Amendments

- **Definition of "identifier"**

As currently drafted, the definition for "Identifier" does not protect the privacy of individuals who provide a landline number on records and/or documents that would fall under the definition of "Specific data element." By deleting the word "mobile" in the definition of "Identifier," page 1, line 21, and simply stating "a phone number" it will protect all individuals who provide a phone number, whether it be a mobile or a landline number, in combination with one or more specific data elements.

- **Definition of "specified data element"**

Hawaii also has a significant military presence, and servicemembers in the State may use their military identification numbers while doing business in Hawaii. The Department recommends adding language at page 2, line 20, to include "military identification numbers" under the definition of "specified data element." This addition will protect the privacy of servicemembers in Hawaii who use their military identification numbers.

Thank you for the opportunity to testify on this bill.

JOSH GREEN, M.D.
GOVERNOR
KE KIA'ĀINA

RYAN I. YAMANE
DIRECTOR
KA LUNA HO'OKELE

JOSEPH CAMPOS II
DEPUTY DIRECTOR
KA HOPE LUNA HO'OKELE

TRISTA SPEER
DEPUTY DIRECTOR
KA HOPE LUNA HO'OKELE

LATE

LATE

STATE OF HAWAII
KA MOKU'ĀINA O HAWAI'I
DEPARTMENT OF HUMAN SERVICES
KA 'OIHANA MĀLAMA LAWELAWE KANAKA
Office of the Director
P. O. Box 339
Honolulu, Hawaii 96809-0339

February 18, 2025

TO: The Honorable Senator Jarrett Keohokalole, Chair
Senate Committee on Commerce and Consumer Protection

FROM: Ryan I. Yamane, Director

SUBJECT: **SB 1038 – RELATING TO PRIVACY.**

Hearing: Wednesday, February 19, 2025, 9:30 a.m.
Conference Room 229 & Videoconference, State Capitol

DEPARTMENT'S POSITION: The Department of Human Services (DHS) appreciates the intent of the measure and provides comments. DHS will need time to assess the resources and time frames needed to implement this measure. For example, we will need to review and update our notices across programs. DHS respectfully requests that the effective date of this bill be extended.

PURPOSE: This 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 among the businesses deemed compliant with security breach notice requirements under existing state law.

Thank you for the opportunity to testify in strong support of this measure.

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Southwest | Telephone 909.380.2783
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetSW

February 17, 2025

Senator Jarrett Keohokalole
Chair, Commerce and Consumer Protection Committee
Hawaii State Capitol
415 South Beretania Street, Room 205
Honolulu, HI 96813

Senator Carol Fukunaga
Vice Chair, Commerce and Consumer Protection Committee
Hawaii State Capitol
415 South Beretania Street, Room 216
Honolulu, HI 96813

Dear Chair Keohokalole, Vice Chair Fukunaga and Members of the Committee,

TechNet must respectfully oppose SB 1038 (Lee), a bill that attempts to modernize the state's data breach notification requirements but that may have some unintended consequences.

TechNet is the national, bipartisan network of technology CEOs and senior executives 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 4.5 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, 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.

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.

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

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 or concerns regarding our position, please contact Jose Torres, Deputy Executive Director at jtorres@technet.org or 909-380-2783.

Sincerely,

Jose Torres, MPA
Deputy Executive Director for California and the Southwest

SanHi
GOVERNMENT STRATEGIES
A LIMITED LIABILITY LAW PARTNERSHIP

DATE: February 17, 2025

TO: Senator Jarrett Keohokalole
Chair, Committee on Commerce and Consumer Protection

FROM: Mihoko Ito / Tiffany Yajima

RE: **S.B. 1038 - Relating to Privacy**
Hearing Date: Wednesday, February 19, 2025 at 9:30 a.m.
Conference Room 229 & Videoconference

Dear Chair Keohokalole, Vice Chair Fukunaga and Members of the Committee on Commerce and Consumer Protection:

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.1038, 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:

First Hawaiian Center T 808-539-0400
999 Bishop Street, Suite 1400 F 808-533-4945
Honolulu, HI 96813 governmentaffairs@awlaw.com

> "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 4, line 20- page 5, line 2 as follows:

> "Personal information does not include publicly available information that is lawfully made available to the public ~~**from federal, state, or local government records**~~.

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.

LATE

February 17, 2025

Senator Jarrett Keohokalole
Chair, Committee on Commerce and Consumer Protection

Re: S.B. 1038: Revised definition of Personal Information (Oppose unless Amended)

Dear Chair Keohokalole, Vice Chair Fukunaga, and members of the Committee on Commerce and Consumer Protection,

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 1038 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. 1038 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."

RELX

london.biggs@relx.com
www.relx.com

Thank you for your consideration of RELX concerns pertaining to S.B. 1038. 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

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

LATE

LATE

February 19, 2025

Senator Jarrett Keohokalole, Chair
Senator Carol Fukunaga, Vice Chair
and members of the Senate Committee on Commerce & Consumer Protection
Hawaii State Capitol
Honolulu, Hawaii 96813

Re: **S.B. 1038 (Privacy)**
Hearing Date/Time: Wednesday, February 19, 2025, 9:30 a.m.

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

The HFSA **opposes this 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 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 4, lines 9 through 20.)

On page 3, line 2 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."

---

[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. 11-15, 15-4, 134-83, 232-7, 232-16, 232-18, 329D-4, 388-11.5, 487D-2, 576D-10.5, and 803-6.

BELOW ARE THE TWO ALTERNATE PROPOSED VERSIONS:

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

(MSCD/hfsa)

STATE PRIVACY & SECURITY COALITION

February 18, 2025

LATE

LATE

Chair Jarrett Keohokalole
Vice Chair Carol Fukunaga
Committee on Commerce and Consumer Protection
Hawaii State Senate
415 South Beretania Street
Honolulu, HI 96817

Re: SB 1038 – Oppose Unless Amended

Dear Chair Keohokalole, Vice Chair Fukunaga, 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 1038 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 if 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

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 1038, 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).

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

SanHi
GOVERNMENT STRATEGIES
A LIMITED LIABILITY LAW PARTNERSHIP

LATE LATE

DATE: February 19, 2025

TO: Senator Jarrett Keohokalole
Chair, Committee on Commerce and Consumer Protection

FROM: Mihoko Ito / Ryan M. Toyomura

RE: **S.B. 1038 - Relating to Privacy**

Dear Chair Keohokalole, Vice Chair Fukunaga and Members of the Committee on Commerce and Consumer Protection:

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. 1038, 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 1038 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.

First Hawaiian Center
999 Bishop Street, Suite 1400
Honolulu, HI 96813
T 808-539-0400
F 808-533-4945
governmentaffairs@awlaw.com

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.

LATE LATE

Hawaii Credit Union League
Your Partner For Success
Unite for Good
1654 South King Street
Honolulu, Hawaii 96826-2097
Telephone: (808) 941.0556
Fax: (808) 945.0019
Web site: www.hcul.org
Email: info@hcul.org

Testimony to the Senate Committee on Commerce and Consumer Protection
February 19, 2025
Conference Room 229

Comments Regarding SB 1038, Relating to Privacy

To: The Honorable Jarrett Keohokalole, Chair
The Honorable Carol Fukunaga, Vice-Chair
Members of the Committee

My name is Stefanie Sakamoto, and I am testifying on behalf of the Hawaii Credit Union League (HCUL), the local trade association for 45 Hawaii credit unions, representing over 877,000 credit union members across the state.

HCUL offers the following comments regarding SB 1038, Relating to Privacy. This 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, and includes licensees subject to the Insurance Data Security Law among the businesses deemed compliant with security breach notice requirements under existing state law.

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 amendments proposed by the Hawaii Financial Services Association.

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