JOSH GREEN, M.D.
GOVERNOR | KE KIAʻĀINA

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIAʻĀINA

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: 1-844-808-DCCA (3222)
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 25, 2026
9:32 a.m.
Conference Room 229

On the following measure:
S.B. 3016, 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 supports this bill.

The purpose of this bill is to update Hawaii's data breach notification law, Hawaii Revised Statutes (HRS) Chapter 487N, by amending the definition of "personal information."

The bill provides a sorely needed update to Hawaii's data breach notification law. With respect to security breaches of personal information occurring at businesses that operate in the State, the core rights created by the data breach notification law are the rights of individuals to receive a notice of security breach from a business in possession of the "personal information" of the individual, and the right of the Office of Consumer

Protection to receive notice from the business about the impact of the breach. Both of these rights, however, are only as valuable as the definition of "personal information," and the definition of "personal information" needs to be updated. This bill aims to rectify the current law, which would be an important step forward in protecting the privacy of Hawaii residents.

We oppose the exemption at Page 6, lines 11-12, for insurance licensees, which would remove individuals' right to receive notice of a security breach that impacts them when the security breach occurs at an insurance licensee. The Insurance Data Security Law, HRS chapter 431B:3B, article 3, does not independently require that notice of a security breach be provided to individuals affected. Only chapter 487N requires that notice of a security breach be provided to individuals affected by a security breach. The Insurance Data Security Law also mandates that licensees comply with chapter 487N. See HRS section 431:3B-303 (setting forth requirements for "Notification to consumers" and mandating that licensees comply with chapter 487N). The existing requirements were clearly intentional because, as mentioned above, only the data breach notification law creates the core right of individuals to receive notification.

We respectfully request the Committee pass this bill with an amendment deleting the new language that appears at Page 6, lines 11-12, that exempts insurance licensee from having to provide notice to individuals affected by a data breach.

Thank you for the opportunity to testify on this bill.

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: 1-844-808-DCCA (3222)
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

Before the
Senate Committee on Commerce and Consumer Protection
Wednesday, February 25, 2026
9:32 a.m.
State Capitol, Conference Room 229 and via Videoconference

On the following measure:
S.B. 3016, RELATING TO PRIVACY

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

My name is Scott K. Saiki, and I am the Insurance Commissioner of the Department of Commerce and Consumer Affairs' (Department) Insurance Division. The Department offers comments on this measure.

The purpose of the measure is to add definitions of "identifier" and "specified data element" and amend 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. The measure includes licensees subject to the Insurance Data Security Law among the businesses deemed compliant with security breach notice requirements.

S.B. 3016 amends subsection 487N-2(g), Hawaii Revised Statutes (HRS) by adding the language, "(3) Any licensee that is subject to the Insurance Data Security Law, chapter 431, article 3B." The Department has concerns that this proposed language may lead to confusion and statutory interpretation issues. With respect to

consumer notices, the Insurance Data Security Law, HRS § 431:3B-303 requires that notices be provided in accordance with HRS § 487N. The proposed amendments to HRS § 487N-2(g) do not appear to account for this and appears to erroneously presume that the Insurance Data Security Law includes its own process for consumer notification. Therefore, the proposed amendment would likely be interpreted by insurance licensees that they are not statutorily required to issue consumer notices.

In light of this, the Department requests that language in S.B. 3016 on page 6, lines 11-12 be deleted.

Thank you for the opportunity to testify on this measure.

LATE

Hawaiian Telcom

Written Statement of

Jeannine Souki,
Senior Manager – Government & Regulatory Affairs

SENATE COMMITTEE ON COMMERCE & CONSUMER PROTECTION
February 25, 2026, 9:32 AM
State Capitol, Conference Room 229 & Videoconference

COMMENTS AND REQUEST TO AMEND:

S.B. 3016 – RELATING TO PRIVACY

To: Chair Keohokalole, Vice Chair Fukunaga, and Members of the Committee
Re: Testimony providing comments and requesting clarifying amendments for SB 3016

Aloha Honorable Chair, Vice-Chair, and Members of the Committee:

Mahalo for the opportunity to provide **comments on SB3016**, which updates Hawai‘i’s data breach-notification law by adding new definitions of “identifier” and “specified data element,” and expanding the scope of “personal information.” Hawaiian Telcom supports efforts to strengthen consumer privacy and modernize Hawai‘i’s breach laws.

We respectfully request a clarifying amendment to ensure the bill does not create **duplicative or conflicting requirements** for telecommunications carriers already regulated under **federal Customer Proprietary Network Information (CPNI) rules (47 U.S.C. § 222)**. While SB3016 provides **deemed-compliance status** for entities regulated under the **Insurance Data Security Law**, it does not extend similar treatment to carriers that must meet robust federal privacy and breach-notification obligations.

Without alignment, carriers will be subjected to **parallel—and potentially conflicting—notice requirements** from single incident, particularly where an event involves both CPNI-regulated data and the expanded categories of “personal information” included in this bill.

Hawaiian Telcom respectfully requests a **clarifying amendment to SECTION 3**, which **amends Section 487N-2, Hawai‘i Revised Statutes**, by amending subsection (g) to specify which entities are deemed in compliance with the section. The proposed language would add telecommunications carriers—regulated under 47 U.S.C. § 222 and 47 C.F.R. Part 64—to the existing list of entities already governed by comprehensive federal privacy and breach-notification requirements, including financial institutions, HIPAA-regulated health providers and health plans, and licensees subject to the Insurance Data Security Law.

Proposed amendment to Section 487N-2, Hawai‘i Revised Statutes, (g):

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

(1) A financial institution that is subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice published in the Federal Register on March 29, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to title 12 [C.F.R. Part] Code of Federal Regulations part 748, and any revisions, additions, or substitutions relating to the interagency guidance; [and]

(2) Any health plan or [healthcare] health care provider that is subject to and in compliance with the standards for privacy or 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[.]; and

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

(4) Any telecommunications carrier that is subject to and in compliance with 47 U.S.C. § 222 and 47 C.F.R. Part 64.

This clarification ensures that consumers continue to receive timely and clear notifications, while preventing duplicative or conflicting reporting obligations for entities already subject to strict federal standards.

Hawaiian Telcom appreciates the Committee’s efforts to strengthen privacy protections and respectfully requests adoption of this amendment to maintain alignment with existing federal requirements.

Mahalo for your consideration.

SanHi
GOVERNMENT STRATEGIES
A LIMITED LIABILITY LAW PARTNERSHIP

DATE: February 24, 2026

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

FROM: Mihoko Ito / Chris Delaunay

RE: **S.B. 3016 - Relating to Privacy**
Hearing Date: Wednesday, February 25, 2026, at 9:32 a.m.
Conference Room: 229

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. 3016, 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.

Perhaps most concerning, while the bill exempts some redacted identifiers, it is not applied uniformly across broader categories of identifiers and newly defined specific data elements. As drafted, S.B. 3016 significantly expands the scope of reportable information and may require breach notification even in circumstances where the practical risk of identity theft or consumer harm is minimal.

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.

First Hawaiian Center
999 Bishop Street, Suite 1400
Honolulu, HI 96813

T 808-539-0400
F 808-533-4945

Hawaii Bankers Association

DATE: February 23, 2026

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

FROM: Mihoko Ito / Tiffany Yajima

RE: **S.B. 3016 - Relating to Privacy**
Hearing Date: Wednesday, February 25, 2026 at 9:32 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. 3016, 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 an amendment we are proposing in this testimony to the definition of the "personal information."

We would recommend that the exclusion for personal 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 6-8 as follows:

> "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 the opportunity to submit this testimony and to offer our proposed amendment. Please let us know if we can provide further information.

808-524-5161 P.O. Box 10065, Honolulu, Hawaii 96816 director@hawaiiba.org

STATE PRIVACY & SECURITY COALITION

February 23, 2026

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

Re: SB 3016 – Relating to Privacy

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

The State Privacy & Security Coalition (SPSC), a coalition of over 30 companies and seven trade associations across the retail, technology, telecommunications, payment card, and healthcare sectors, appreciates the opportunity to provide testimony on Senate Bill 3016.

SPSC supports thoughtful updates to Hawaii's breach notification framework to account for evolving technologies and data practices. As drafted, however, SB 3016 expands key definitions in ways that depart from nationally adopted standards and extend beyond data elements that meaningfully increase the risk of identity theft or consumer fraud. Several provisions are overbroad and may trigger notification in circumstances where no material risk exists. Expansive or unclear triggers can lead to consumer confusion and dilute the practical value of breach notices by signaling heightened danger where the underlying facts do not warrant it.

Our proposed amendments preserve the expanded list of Hawaii data elements, including financial account information, while ensuring that notification obligations remain focused on incidents that reasonably place consumers at risk. We offer these recommendations with the goal of helping ensure the legislation achieves its objectives in a clear, targeted, and workable manner.

I. THE BILL SHOULD PRESERVE THE TRADITIONAL NAME-PLUS-DATA ELEMENT APPROACH

SB 3016 replaces the longstanding formulation of "personal information" (e.g., an individual's first name or first initial and last name in combination with specified sensitive data elements) with a new standalone "identifier" category. That category includes usernames, phone numbers, and email addresses. Every other state continues to rely on the traditional name-plus-data-element approach in its breach notification statute.[1] Hawaii may reasonably expand the list of covered sensitive data elements, but doing so should not require departure from a framework that is uniform across jurisdictions.

[1] *See, e.g.,* Cal. Civ. Code § 1798.82(h)(1); N.Y. Gen. Bus. Law § 899-aa(a); Tex. Bus. & Com. Code Ann. § 521.002(a)(1); 815 Ill. Comp. Stat. 530/5; Va. Code Ann. § 18.2-186.6(A); Fla. Stat. § 501.171(1)(g) (each defining covered information through the association of an individual's name with enumerated sensitive data elements).

Alignment across states remains critical in the breach notification context. Multi-state incidents require rapid legal assessment and coordinated notice to affected individuals. When statutory definitions are consistent, businesses can determine notification obligations efficiently and provide timely notice. A Hawaii-specific construct would require separate analysis for Hawaii residents, increasing operational complexity and potentially delaying notification.

Concern also arises from the "common piece of information" included within the proposed "identifier" definition. Phone numbers and email addresses are widely available and, in many instances, publicly accessible. Treating those data points as the foundational trigger for breach notification would substantially broaden the scope of reportable incidents without a corresponding increase in identity theft or fraud risk. Consumers could receive notices suggesting heightened danger where no material risk exists. For example, if an unauthorized actor obtains an unencrypted driver's license number, the addition of a phone number does not materially increase the individual's risk profile.

Unauthorized access to online account credentials can be addressed through a more targeted amendment, discussed in Section IV below, without restructuring the core elements of Hawaii's breach notification statute.

II. THE BILL SHOULD PRESERVE CLEAR PROTECTION FOR ENCRYPTED OR OTHERWISE UNUSABLE INFORMATION

Under current Hawaii law, encrypted data is appropriately treated as posing reduced risk. When information is accessed without authorization but remains encrypted or otherwise protected, and the encryption key has not been compromised, the likelihood of harm to a Hawaii resident is materially diminished. 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.

III. THE BILL SHOULD COMBINE FINANCIAL ACCOUNT NUMBERS WITH ACCESS CREDENTIALS

Under SB 3016, "specified data element" separately lists an individual's financial account number or credit or debit card number and, in a different subsection, a security code, access code, personal identification number, or password that would allow access to an individual's account. Separating those elements risks expanding breach notification triggers beyond circumstances that meaningfully increase the risk of fraud.

Financial harm generally arises when an unauthorized actor obtains both the account number and the credentials necessary to access the account. Treating those elements independently could require notification where an access credential is obtained without the corresponding account number, or vice versa, even though no practical ability to access funds exists.

Nearly all states pair financial account numbers with the access information required to use them, limiting reportable incidents to combinations that enable account access.[2] Aligning Hawaii's statute with that approach would clarify that reportable incidents involve combinations of data that create material risk, rather than isolated data points.

Accordingly, subsections (5) and (6) should be combined to read: "An individual's financial account number, or credit card or debit card number, in combination with any security code, access code, personal identification number, or password that would allow access to the individual's account."

IV. THE BILL SHOULD AMEND THE DEFINITION OF "PERSONAL INFORMATION"

As drafted, SB 3016 would make Hawaii an outlier among other states by requiring a formal breach notification process where there are attempts to access a consumer's online account. Other states have instead developed an approach that permits rapid notification in the ordinary course of the consumer's interaction with the business.[3] Many consumers routinely receive emails encouraging them to change passwords or review account activity following suspicious login attempts.

Although our proposed amendments are tailored to the confines of SB 3016, we would support including an additional definition under "Personal Information," consistent with language adopted in other states, to read as follows:

> "Personal information" means **either: (i)** an individual's first initial or first name and last name, in combination with one or more specified elements, when the personal information is not encrypted, redacted, or otherwise protected by a 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.**

[2] *See, e.g.*, Colo. Rev. Stat. § 6-1-716(g)(I)(A); Conn. Gen. Stat. § 36a-701b(2)(vi); AL Code § 8-38-2(2)(6)(3); Del. Code Ann. tit. 6 § 12B-101(7)(3); Nev. Rev. Stat. § 603A.040(1)(c) (each defining covered information to include financial account or payment card numbers when combined with security codes, access codes, PINs, or passwords permitting account access).

[3] *See, e.g.*, MS Code § 75-24-29 ("(1) This section applies to any person who conducts business in this state and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any resident of this state."); Wis. Stat. Ann. § 134.98(1)(a)(1) (defining "entity" as a person, other than an individual, that "[c]onducts business in this state and maintains personal information in the ordinary course of business").

These provisions allow consumers to be notified promptly when there is suspicious activity involving account credentials and to receive notice in a secure manner. The second clause ensures that, if a consumer's email account has been compromised, a business does not send a password reset link to that same compromised address.

We appreciate the time and effort the Committee has devoted to this legislation and thank you for your consideration of our comments. Please do not hesitate to contact us with any questions or concerns.

Respectfully submitted,

Andrew A. Kingman
Counsel, State Privacy & Security Coalition

William C. Martinez
Counsel, State Privacy & Security Coalition

SB-3016
Submitted on: 2/20/2026 7:34:18 PM
Testimony for CPN on 2/25/2026 9:32:00 AM

Submitted By	Organization	Testifier Position	Testify
Johnnie-Mae L. Perry	Individual	Support	Written Testimony Only

Comments:

I, Johnnie-Mae L. Perry, Support

3016 SB RELATING TO PRIVACY.

SB-3016
Submitted on: 2/23/2026 5:29:06 PM
Testimony for CPN on 2/25/2026 9:32:00 AM

Submitted By	Organization	Testifier Position	Testify
Michael Olderr	Individual	Support	Written Testimony Only

Comments:

I support this bill. Everyone has access to cash, to a dollar, if they are ready to spend it. Cash cannot fail if your phone's battery has died, if there is a problem with the bank, or if your cryptocurrency goes under. Digital assets are fine, but replacing physical currency with them will be disastrous for everyone.