DAVID Y. IGE
GOVERNOR

JOSH GREEN
LT. GOVERNOR

STATE OF HAWAII
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS
335 MERCHANT STREET, ROOM 310
P.O. BOX 541
HONOLULU, HAWAII 96809
Phone Number: 586-2850
Fax Number: 586-2856
cca.hawaii.gov

CATHERINE P. AWAKUNI COLÓN
DIRECTOR

JO ANN M. UCHIDA TAKEUCHI
DEPUTY DIRECTOR

Testimony of the Department of Commerce and Consumer Affairs

Before the
Senate Committee on Commerce and Consumer Protection
Wednesday, February 17, 2021
9:30 a.m.
Via Videoconference

On the following measure:
S.B. 1100, RELATING TO INSURANCE DATA SECURITY

Chair Baker and Members of the Committee:

My name is Colin Hayashida, and I am the Insurance Commissioner of the Department of Commerce and Consumer Affairs' (Department) Insurance Division. The Department supports this administration bill.

The purpose of this bill is to adopt the National Conference of Insurance Commissioners' (NAIC) Insurance Data Security Model Law to establish insurance data security standards for Hawaii insurance licensees.

The NAIC adopted the Data Security Model Law in 2017 to strengthen existing data privacy standard and consumer breach notification obligations of insurance licensees. If this bill does not pass by 2022, states may risk federal preemption of state laws in this area. Although some licensees may already have cybersecurity policies and protocols in place, this bill will ensure and formalize insurance data security protections for all insurance licensees.

Thank you for the opportunity to testify, and we respectfully ask the Committee to pass this administration bill.

HAWAII INSURERS COUNCIL
A trade association of property and casualty insurance companies

Pauahi Tower, Suite 2010
1003 Bishop Street
Honolulu, Hawaii 96813
Telephone (808) 525-5877

Alison H. Ueoka
President

TESTIMONY OF ALISON UEOKA

COMMITTEE ON COMMERCE AND CONSUMER PROTECTION
Senator Rosalyn H. Baker, Chair
Senator Stanley Chang, Vice Chair

Wednesday, February 17, 2021
9:30 a.m.

SB 1100

Chair Baker, Vice Chair Chang, and members of the Committee on Commerce and Consumer Protection, my name is Alison Ueoka, President of the Hawaii Insurers Council. The Hawaii Insurers Council is a non-profit trade association of property and casualty insurance companies licensed to do business in Hawaii. Member companies underwrite approximately forty percent of all property and casualty insurance premiums in the state.

Hawaii Insurers Council submit comments on this bill. SB 1100 creates a new article, "Article A Insurance Data Security Law." We respectfully request two amendments, the first on page 15, line 11 under Section 431:A-I(a). We ask that the annual certification be submitted by March 31 instead of February 15 which would better align with existing deadlines for other annual filings required of domestic insurers.

The second amendment we request is on page 17, line 9 under Section 431:A-K(a). We ask that the notification of a cybersecurity event to the commissioner be no later than three business days rather than seventy-two hours to allow the licensee more time to focus on mitigating the breach and in the event the breach occurs near or on a weekend.

Thank you for the opportunity to testify.

TESTIMONY OF THE AMERICAN COUNCIL OF LIFE INSURERS
COMMENTING ON SB 1100, RELATING TO INSURANCE DATA SECURITY

February 17, 2021

Honorable Senator Rosalyn H. Baker, Chair
Committee on Commerce and Consumer Protection
State Senate
Hawaii State Capitol, Room 229 & Video-Conference
415 South Beretania Street
Honolulu, Hawaii 96813

Chair Baker and Members of the Committee:

Thank you for the opportunity to comment on SB 1100, Relating to Insurance Data Security.

Our firm represents the American Council of Life Insurers ("ACLI"). The American Council of Life Insurers (ACLI) is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 280 member companies represent 94% of the industry assets in the United States. Two hundred eighteen (218) ACLI member companies currently do business in the State of Hawaii; and they represent 94% of the life insurance premiums and 99% of the annuity considerations in this State.

SB 1100 adopts the National Association of Insurance Commissioners'("NAIC") Insurance Data Security Model Act which establishes insurance data security standards for life insurers licensed to do business in this state.

While ACLI and its member companies support Hawaii's adoption of the NAIC Model Act we request your consideration of our suggested revisions to SB 1100 as set forth below.

We suggest that the committee amend §431:A-K(d), on page 20, after line 10 of the bill (which requires an insurer to update and supplement initial and subsequent notifications to the commissioner of a cybersecurity event), as follows:

> (d) The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner regarding material changes to previously provided information relating to the cybersecurity event.

This amendment will eliminate the necessity of an insurer having to update and supplement minor changes in its previous notifications to the commissioner involving the cybersecurity event.

Further, ACLI suggests that SB 1100 be amended by adding a new section §431:A-T-1, to be inserted immediately following section § 431:A-T, on page 28, after line 11 of the bill, to read as follows:

> **§431:A-T Private cause of action**. This article may not be construed to create or imply a private cause of action for violation of its provision, and it may not be construed to curtail a private cause of action that would otherwise exist in the absence of this article.
>
> **§ 431:A-T-1** Exclusive data security standards. Notwithstanding any other provision of law, this Article establishes the exclusive state standards applicable to Licensees for data security, the investigation of a Cybersecurity Event as defined in Section 3, and notification to the Commissioner.

The proposed amendment would clarify that the data security standard established by the new article and not others which may be established in the future shall be the governing law applicable to insurers

Thank you for your consideration of our proposed amendments and the opportunity to comment on SB 1100, Relating to Insurance Data Security.

LAW OFFICES OF
OREN T. CHIKAMOTO
A Limited Liability Law Company

Oren T. Chikamoto
1001 Bishop Street, Suite 1750
Honolulu, Hawaii 96813
Telephone: (808) 531-1500
E mail: otc@chikamotolaw.com

NAMIC
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

317.875.5250 | [F] 317.879.8408
3601 Vincennes Road, Indianapolis, Indiana 46268

202.628.1558 | [F] 202.628.1601
20 F Street N.W., Suite 510 | Washington, D.C. 20001

Hawaii State Legislature
Senate Committee on Commerce and Consumer Protection

February 16, 2021

Filed via electronic testimony submission system

RE: SB 1100, Relating to Insurance Data Security - NAMIC's Testimony

Thank you for providing the National Association of Mutual Insurance Companies (NAMIC) an opportunity to submit written testimony to your committee for the February 17, 2021 public hearing. Unfortunately, I will not be able to attend the public hearing, because of a previously scheduled professional obligation. NAMIC's written comments need not be read into the record, so long as they are referenced as a formal submission and are provided to the committee for consideration.

The National Association of Mutual Insurance Companies is the largest property/casualty insurance trade group with a diverse membership of more than 1,400 local, regional, and national member companies, including seven of the top 10 property/casualty insurers in the United States. NAMIC members lead the personal lines sector representing 66 percent of the homeowner's insurance market and 53 percent of the auto market. NAMIC has 84 members who write property/casualty in the State of Hawaii, which represents 28% of the insurance marketplace.

NAMIC respectfully submits the following comments:

1) **Proposed Change to "Purpose and Intent" Section of the bill:**

NAMIC believes that it makes sense to move the "Justification Sheet" public policy statement to the body of the "Act" so that it is clear that the key provisions contained in the "Justification Sheet' are legally controlling and operational. The National Conference of Insurance Commissioners (NAIC) Model creates model standards for "data security," but it is not authoritative. Since state law is controlling it is imperative that the "Act' be organized and worded so as to prevent any opportunity for overlapping and/or dual regulation. Thus, we recommend language to prevent insurers and other licensees from being exposed to multiple, sometimes inconsistent, state law requirements.

NAMIC respectfully recommends the following revision: (underlined text denotes suggested additions to current language)

Purpose and Intent

(a) *To establish the exclusive standards for data security and for the investigation of and notification to the Commissioner of a cybersecurity event applicable to Licensees, as defined in Section §431:A-A. If another law in this state requires a Licensee to provide notice to another regulator in this state, the Licensee may satisfy that requirement by providing notice to the regulator in compliance with Section §431:A-K of this Act.*

(b) This Act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

2) Proposed revisions to "Definitions" Section of the bill:

- Page 2, *line* 3: The bill defines "cybersecurity event" needlessly and inappropriately too broadly. NAMIC recommends clarifying the language to apply it to only nonpublic information that is being protected. We suggest the following revision:

  "Cybersecurity event" means an event resulting in unauthorized access to, disruption or misuse of, an information system or nonpublic information stored on that information system. "Cybersecurity event" shall not include:

- Page 3, *line*. 1: NAMIC believes that the "Information System" definition should be similarly restricted. We suggest the following revision:

  "Information system" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic nonpublic information, as well as any specialized system such as industrial controls systems, process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

- Page 3, *line* 21 – Page 4, *line*. 19: We think the definition of "nonpublic information" should be limited to electronic information; after all, that is what is being addressed in the legislation. Also, the bill's definition includes a licensee's business-related information, which is unnecessary and excessive. The purpose of the bill is to protect consumer "nonpublic" information. Therefore, we suggest the following revisions, which better tailor the definition to the stated public policy objective of the bill:

  "Nonpublic information" means electronic information that is not publicly available information and is:

(1) ~~Business-related information of a licensee, whose tampering, unauthorized disclosure, access, or use would cause a material adverse impact to the business, operations, or security of the licensee; or~~

(2) (C) Financial account number, credit, or debit card number;

(3) Any information or data subject to Pub. L. 104-191, 110 Stat. 1936, enacted August 21, 1996 (Health Insurance Portability and Accountability Act), except age or gender, in any form or medium created by or derived from a health care provider or a consumer that identifies a particular consumer and that relates to:

3) NAMIC believes that various provisions of the Model Law should be revised to recognize the unique nature of Third-Party Service Provider agreements regarding cloud services. Consequently, we offer the following suggested revisions:

- Page 13, *lines* 13-17 - **§431:A-F Oversight of third-party service provider arrangements**. A licensee shall:

(1) Exercise due diligence in selecting its third—party service provider; and

(2) Where appropriate, require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to or held by the third-party service provider. Encrypted nonpublic information is not accessible to, or held by, the third-party service provider within the meaning of this section if the third-party service provider does not possess the associated protective process or key necessary to assign meaning to the nonpublic information.

- Page 16, *lines* 20-22:

(b) *If the licensee **provides nonpublic information to a third-party service provider and** learns that a cybersecurity event has or may have ~~occurred~~ **impacted the licensee's nonpublic information** in a system maintained by a third-party service provider, the licensee will complete the steps listed in subsection (b) or confirm and document that the third-party service provider has completed those steps.*

- Page 21, *line* 20 – Page 22, *line*. 2:

> **§431:A-M Notice regarding cybersecurity events of third-party service providers.**
>
> *(a) In the case of a cybersecurity event impacting a licensee's nonpublic information in a system maintained by a third—party service provider, of which the licensee has become aware, the licensee shall treat the event as it would under section 43le-K unless the third-party service provider provides the notice required under section 43le-K to the Commissioner.*

4) **Notice of Cybersecurity Event** - Section 431:A-K requires Licensees to provide notice of a Cybersecurity Event to the Insurance Commissioner. NAMIC is concerned that these requirements might shift the licensee's focus from containing the incident for the protection of the consumer, which would undermine the very purpose of the law. In addition, the proposed requirements could conflict with law enforcement instructions, and might place different requirements on independent contractor agents than it does for exclusive insurer agents. This presents a challenge given because these incidents are likely to be handled in both instances by a centralized team.

Consequently, NAMIC offers the following suggested revisions:

- Page 17, *line* 7 – Page 18, *line* 7:

> ***§431:A-K Notification of a cybersecurity event.*** *(a) Each licensee shall notify the commissioner as promptly as possible, but in no event later than ~~seventy-two hours~~ three business days from a determination that a cybersecurity event impacting 250 or more consumers has occurred. If law enforcement officials instruct a Licensee not to distribute information regarding a Cybersecurity Event, the Licensee shall not be required to provide notification until instructed to do so by law enforcement. Notification shall be provided~~,~~ when either of the following criteria has been met:*
>
> *(1) This State is the licensee's state of domicile, in the case of an insurer, or this State is the licensee's home state, in the case of ~~a~~ an independent insurance producer; or*
>
> *(2) The licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in this State and ~~that~~ is ~~either of the following:~~*

~~*(A) A cybersecurity event impacting the licensee, in which notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body pursuant to any state or federal law; or*~~

~~*(B) A*~~ *a cybersecurity event that has a reasonable likelihood of materially harming:*

~~*(i)*~~ *(A) Any consumer residing in this State; or*
~~*(ii)*~~ *(B) Any material part of the normal operation of the licensee.*

5) **Regulatory Oversight** - NAMIC supports an amendment permitting a licensee's domiciliary regulator, rather than the regulator from the state enacting the Model to have examination authority for cyber issues. Allowing each individual state to have the authority to examine could expose insurers to contradictory conclusions and directions on cyber issues, and place a large administrative burden on the licensee's information security functions, ultimately shifting their focus from protecting customer information to responding to a multitude of state regulatory requests. This is especially true of a potential cyber breach, which could extend across multiple state lines and expose a licensee to inconsistent actions based on the same cyber event. To address this logistical concern, NAMIC suggests that this regulatory authority exclusively reside with the licensee's domiciliary regulator in the context of a financial examination.

Consequently, NAMIC recommends the following revisions:

- Page 24, *lines* 1 – 17:

§431:A-P Powers of the commissioner. *(a) The* ***licensee's domiciliary*** ~~*commissioner*~~ ***regulator*** *shall have power to examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this article.*

(b) ~~*This power is in addition to the powers that the commissioner has under section 431:2-208.*~~ *Any investigation or examination* ***of a Hawaii-domiciled licensee*** *shall be conducted pursuant to section 431:2-301.7.*

6) **Breach notification to be sent to the Commissioner** – Since the proposed legislation would require an insurer to provide notice to the Commissioner within 72 hours of discovering a breach, it is unlikely that an insurer would have all the information necessary to satisfy the specific content reporting

requirements of this section. NAMIC suggests the following revisions that recognize the practical realities of an evolving cybersecurity situation and which provide insurers with reasonable flexibility they need to handle the event and protect their consumers.

Consequently, NAMIC suggests the following revisions:

- Page 19, *lines* 8-9; Page 20, *lines* 10-12:

  §431:A-K Notification of a cybersecurity event.

  (b) The licensee shall provide as much of the following information as possible and practicable as promptly as possible:

  (d) The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner regarding material changes to previously provided information concerning the cybersecurity event.

- Page 20, *lines* 15-19

  §431:A-L Notification to consumers.

  The licensee shall comply with chapter 487N, as applicable, and provide a copy of the notice sent to consumers under that chapter to the commissioner if that statute requires a licensee to provide the consumer a paper notice, when a licensee is required to notify the commissioner under section 431A-K.

7) **Inclusion of a Safe Harbor –** NAMIC supports inclusion of a reasonable and appropriate statutory affirmative defense to civil legal actions brought against insurers following a cybersecurity event for licensees who are in compliance with the model's standards.

Suggested inclusions in proposed legislation:

- *A licensee that satisfies the conditions of this article may assert that compliance as an affirmative defense to any cause of action brought under the laws of this state or in the courts of this state alleging that the failure to implement reasonable information security controls resulted in a cybersecurity event concerning nonpublic information.*

- *The affirmative defense permitted under this section shall not limit any other affirmative defenses available to a licensee.*

Alternative legislative approach on affirmative defense – a separate statute: NAMIC would also support an approach such as that used in Ohio (Senate Bill 220, effective Nov. 2, 2018), which enacted a separate statute that creates a broader affirmative defense for entities in breach situations. The Ohio statute, designed to provide an incentive to businesses to protect against data breaches, provides a safe harbor for an organization with a cybersecurity program that conforms to reasonable "industry-recognized" cybersecurity frameworks.

Thank you for your time and consideration. Please feel free to contact me at 303.907.0587 or at crataj@namic.org, if you would like to discuss NAMIC's written testimony.

Respectfully,

Christian John Rataj, Esq.
NAMIC Senior Regional Vice President
State Government Affairs, Western Region