

Version 1.2

*New Model – Privacy Protections Working Group  
Draft: 7/11/2023*

**INSURANCE CONSUMER PRIVACY PROTECTION MODEL LAW**

**Table of Contents**

<b>ARTICLE I.</b>	<b>GENERAL PROVISIONS</b> .....	<b>2</b>
Section 1.	Purpose and Scope .....	2
Section 2.	Definitions .....	3
Section 3.	Oversight of Third-Party Service Provider Arrangements.....	12
Section 4.	Data Minimization .....	13
Section 5.	Sharing Limitations .....	13
Section 6.	Consumers’ Consent .....	16
Section 7.	Retention and Deletion of Consumers’ Information .....	17
<b>ARTICLE III.</b>	<b>NOTICES AND DELIVERY OF NOTICES</b> .....	<b>19</b>
Section 8.	Notice of Consumer Privacy Protection Practices .....	19
Section 9.	Content of Consumer Privacy Protection Practices Notices .....	20
Section 10.	Notice of Consumer Privacy Rights.....	22
Section 11.	Delivery of Notices Required by This Act.....	22
<b>ARTICLE IV.</b>	<b>CONSUMERS’ RIGHTS</b> .....	<b>24</b>
Section 12.	Access to Personal and Publicly Available Information.....	24
Section 13.	Correction or Amendment of Personal or Publicly Available Information .....	25
Section 14.	Adverse Underwriting Decisions .....	26
Section 15.	Nondiscrimination and Nonretaliation .....	27
<b>ARTICLE VI.</b>	<b>ADDITIONAL PROVISIONS</b> .....	<b>28</b>
Section 16.	Investigative Consumer Reports.....	28
Section 17.	Compliance with HIPAA and HITECH.....	29
<b>ARTICLE VII</b>	<b>GENERAL PROVISIONS</b> .....	<b>29</b>
Section 18.	Power of Commissioner .....	29
Section 19.	Confidentiality.....	29
Section 20.	Record Retention.....	31
Section 21.	Hearings, Records, and Service of Process .....	31
Section 22.	Service of Process -Third-Party Service Providers .....	31
Section 23.	Cease and Desist Orders and Reports .....	32
Section 24.	Penalties.....	32
Section 25.	Judicial Review of Orders and Reports.....	32
Section 26.	Individual Remedies .....	33
Section 27.	Immunity .....	33
Section 28.	Obtaining Information Under False Pretenses .....	33
Section 29.	Severability .....	33
Section 30.	Conflict with Other Laws .....	33
Section 32.	Rules and Regulations.....	34
Section 33.	Effective Date and Compliance Dates .....	34

Version 1.2

ARTICLE 1. GENERAL PROVISIONS

Section 1. Purpose and Scope

- A. The purpose of this Act is to establish (i) standards for the collection, processing, retaining, or sharing of consumers' personal information by licensees and their third-party service providers to maintain a balance between the need for information by those in the business of insurance and consumers' need for fairness and protection in the use collection, processing, retaining, or sharing of consumers' personal information; (ii) standards for licensees engaged in additional activities involving the collection, processing, retaining, or sharing consumers' personal information; and (iii) standards applicable to licensees for providing notice to consumers of the collection, processing, retention, or sharing of consumers' personal and publicly information. These standards address the need to:
- (1) Limit the collection, processing, retention, or sharing of consumers' personal information to purposes and activities required in connection with insurance transactions and additional activities;
  - (2) Enable consumers to know what personal information is collected, processed, retained, or shared;
  - (3) Enable consumers to know the sources from whom consumers' personal information is collected and with whom such information is shared;
  - (4) Enable consumers to understand why and for generally how long personal information is retained;
  - (5) Enable consumers to choose whether to consent to the collection, processing, retaining, or sharing of consumers' personal information by licensees and their third-party service providers for additional activities;
  - (6) Permit individual consumers to access personal information relating to the consumer requesting access, to verify or dispute the accuracy of the information;
  - (7) Permit consumers to obtain the reasons for adverse underwriting transactions;
  - (8) Encourage all licensees and third-party service providers used by licensees to implement data minimization practices in the collection, processing, retaining, or sharing of consumers' personal information; and
  - (9) Provide accountability for the improper collection, processing, retaining, or sharing of consumers' personal information by licensees and any third-party service providers used by licensees in violation of this Act.
- B. The obligations imposed by this Act shall apply to licensees and third-party service providers that on or after the effective date of this Act:
- (1) Collect, process, retain, or share consumers' personal information in connection with insurance transactions;
  - (2) Engage in insurance transactions with consumers; or
  - (3) Engage in additional activities involving consumers' personal information.
- C. The protections granted by this Act shall extend to consumers:

Commented [NJ1]: Based on 670

## Version 1.2

- (1) Whose information is collected, processed, retained, or shared in connection with insurance transactions;
- (2) Who have engaged in the past in insurance transactions with any licensee or third-party service provider; or
- (3) Whose personal information is used in additional activities by licensees and third-party service providers.

**Drafting Note:** This model is intended to replace *NAIC Insurance Information and Privacy Protection Model Act* (#670) and *Privacy of Consumer Financial and Health Information Regulation* (#672). For that reason, it includes the protections for consumers that are currently provided by Models #670 and #672 and adds additional protections that reflect the business practices in the insurance industry today. The business of insurance is more global than it was 30 to 40 years ago. This model law reflects those realities and addresses the need for additional protections for consumers. This model requires notices to consumers for various privacy concerns and will supplant any notices required under Model #670, Model #672 and Gramm-Leach Bliley.

### Section 2. Definitions.

As used in this Act:

A. "Address of record" means:

- (1) A consumer's last known USPS mailing address shown in the licensee's records; or
- (2) A consumer's last known email address as shown in the licensee's records, if the consumer has consented under [refer to the state's UETA statute] to conduct business electronically.
- (3) An address of record is deemed invalid if
  - (a) USPS mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the consumer have been unsuccessful; or
  - (b) The consumer's email address in the licensee's records is returned as "not-deliverable" and subsequent attempts by the licensee to obtain a current valid email address for the consumer have been unsuccessful.

B. "Adverse underwriting decision" means:

- (1) Any of the following actions with respect to insurance transactions involving primarily personal, family, or household use:
  - (a) A denial, in whole or in part, of insurance coverage requested by a consumer;
  - (b) A termination of insurance coverage for reasons other than nonpayment of premium;
  - (c) A rescission of the insurance policy;
  - (d) In the case of a property or casualty insurance coverage:
    - (i) Placement by an insurer or producer of a risk with a residual market mechanism, non-admitted insurer or an insurer that specializes in substandard risks;

**Commented [KJ2]:** Language taken from Model 668 (IDSA)

**Commented [KJ3]:** The language in this subdivision was taken from Model 672.

**Commented [KJ4]:** By limiting AUDs in this manner, we provide consistency with current state law (for those states that adopted Model 670 and consistency with FCRA).

Version 1.2

- (ii) The charging of a higher rate based on information which differs from that which the consumer furnished; or
- (e) In the case of a life, health, or disability insurance coverage, an offer to insure at higher than standard rates.
- (2) Notwithstanding Section 2C(1), the following insurance transactions shall not be considered adverse underwriting decisions but the insurer responsible for the occurrence shall provide the consumer with the specific reason or reasons for the occurrence in writing:
  - (a) The termination of an individual policy form on a class or state-wide basis;
  - (b) A denial of insurance coverage solely because such coverage is not available on a class- or state-wide basis; or
  - (c) If requested by a consumer, any other insurer-initiated increase in premium on an insurance product purchased by a consumer.

**Drafting Note:** The use of the term “substandard” in Section 2 C (1) (d)(i) is intended to apply to those insurers whose rates and market orientation are directed at risks other than preferred or standard risks. To facilitate compliance with this Act, *states* should consider developing a list of insurers operating in their state which specialize in substandard risks and make it known to insurers and producers.

- C. “Affiliate” or “affiliated” means a person that directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with another person. For purposes of this definition “control” means:
  - (1) Ownership, control, or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;
  - (2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or
  - (3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.
- D. “Aggregated consumer information” means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer, household, or specific electronic device.
- E. “Biometric information” means an individual’s physiological, biological, or behavioral characteristics that can be used, singly or in combination with other identifying information, to establish a consumer’s identity. Biometric information may include an iris or retina scan, fingerprint, face, hand, palm, ear, vein patterns, and voice prints, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted; and keystroke patterns or rhythms, gait patterns or rhythm that may be used to identify a consumer.
- F. “Clear and conspicuous notice” means a notice that is reasonably understandable and designed to call attention to the nature and significance of its contents.
- G. “Collect” or “collecting” means buying, renting, gathering, obtaining, receiving, or accessing any consumers’ personal information by any means.
- H. “Commissioner” means [insert the appropriate title and statutory reference for the principal insurance regulatory official of the state].

**Commented [KJ5]:** This language comes from Model 672

**Commented [KJ6]:** Language from Model 672 in part.

**Commented [KJ7]:** Model 672 definition only applies to identified data: *to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information*

Version 1.2

- I. **Consumer** means an individual who is a resident of [State] and the individual's legal representative, whose personal information is used, may be used, or has been used in connection with an insurance transaction, including a current or former (i) applicant, (ii) policyholder, (iii) insured, (iv) participant, (v) annuitant or (vi) certificate holder whose personal information is used, may be used, or has been used in connection with an insurance transaction or other financial transaction.
- (1) A consumer shall be considered a resident of this state if the consumer's last known mailing address, as shown in the records of the licensee, is in this state unless the last known address of record is deemed invalid.
  - (2) A consumer is in an ongoing business relationship with a licensee if there is a continuing relationship between the consumer and the licensee based on one or more insurance transactions provided by the licensee.
- J. "Consumer report" means the same as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).
- K. "Consumer reporting agency" means a person who:
- (1) Regularly engages, in whole or in part, in the practice of assembling or preparing consumer reports for a monetary fee;
  - (2) Obtains information primarily from sources other than insurers; and
  - (3) Furnishes consumer reports to other persons.
- L. "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services.
- M. "Delete" and "deleted" means to remove or destroy personal information by permanently and completely erasing the personal information on existing systems such that it is not maintained in human or machine-readable form and cannot be retrieved or utilized in such form;
- N. "De-identified information" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a licensee that uses de-identified information meets all the following:
- (1) Has implemented technical safeguards designed to prohibit re-identification of the consumer to whom the information may pertain.
  - (2) Has implemented reasonable business policies that specifically prohibit re-identification of the information.
  - (3) Has implemented business processes designed to prevent inadvertent release of de-identified information.
  - (4) Makes no attempt to re-identify the information.
- O. "Financial product or service" means a product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

Commented [KJ8]: This definition is similar to that in Model 672.

Version 1.2

- P. "Genetic information" means:
- (1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:
    - (a) The individual's genetic tests;
    - (b) The genetic tests of family members of the individual;
    - (c) The manifestation of a disease or disorder in family members of such individual; or
    - (d) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.
  - 2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:
    - (a) A fetus carried by the individual or family member who is a pregnant woman; and
    - (b) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.
  - (3) Genetic information excludes information about the sex or age of any individual.

Q. "Health care" means:

- (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, services, procedures, tests, or counseling that:
  - (a) Relates to the physical, mental, or behavioral condition of an individual; or
  - (b) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs, or any other tissue; or
- (2) Prescribing, dispensing, or furnishing drugs or biologicals, or medical devices, or health care equipment and supplies to an individual.

Commented [KJ9]: Taken from Model 672

R. "Health care provider" means a health care practitioner licensed, accredited, or certified to perform specified health care consistent with state law, or any health care facility.

Commented [KJ10]: This definition comes from Model 672

S. "Health information" means any consumer information or data except age or gender, created by or derived from a health care provider or the consumer that relates to:

Commented [KJ11]: This definition comes from Model 672

- (1) The past, present, or future (i) physical, (ii) mental, or (iii) behavioral health, or condition of an individual;
- (2) The genetic information of an individual;
- (3) The provision of health care to an individual; or
- (4) Payment for the provision of health care to an individual.

T. "Institutional source" means any person or governmental entity that provides information about a consumer to a licensee other than:

Commented [KJ12]: Model 670

- (1) A producer;

Version 1.2

- (2) A consumer who is the subject of the information; or
- (3) An individual acting in a personal capacity rather than in a business or professional capacity.

U. "Insurance support organization" means:

**Commented [KJ13]:** Model 670

- (1) Any person who regularly engages in the collection, processing, retention, or sharing of consumers' information for the primary purpose of providing insurers or producers information in connection with insurance transactions, including:
  - (a) The furnishing of consumer reports or investigative consumer reports to licensees or other insurance support organizations for use in connection with insurance transactions;
  - (b) The collection of personal information from licensees or other insurance support organizations to detect or prevent fraud, material misrepresentation, or material nondisclosure in connection with insurance transactions;
  - (c) The collection of any personal information in connection with an insurance transaction that may have application in transactions or activities other than insurance transactions.
- (2) Notwithstanding Subdivision (1) of this subsection, producers, government institutions, insurers, health care providers shall not be considered "insurance support organizations" for purposes of this Act.

V. "Insurance transaction" means any transaction or service by or on behalf of a licensee and its affiliates related to:

**Commented [KJ14]:** Model 672 uses "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.  
(2) Insurance service includes a licensee's evaluation, brokerage or distribution of information that the licensee collects in connection with a request or an application from a consumer for a insurance product or service.

- (1) The underwriting or the determination of a consumer's eligibility for or the amount of insurance coverage, rate, benefit, payment, or claim settlement;
- (2) Licensees or third-party service providers performing services including maintaining or servicing accounts, providing customer service, processing requests or transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, providing similar services or any similar services;
- (3) Provision of "value-added services or benefits" in connection with an insurance transaction;
- (4) Any mathematical-based decision that involves personal information;
- (5) Any actuarial studies related to rating, risk management, or exempt research activities conducted by or for the benefit of the licensee using consumers' personal information;
- (6) Offering, selling, or servicing of a financial product or service of the licensee or its affiliates;
- (7) The short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with the licensee, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the licensee;

Version 1.2

(8) Enabling solely internal uses that are compatible with the context in which the consumer provided the information; or

W. "Insurer" means

- (1) Any person or entity required to be licensed by the commissioner to assume risk, or otherwise authorized under the laws of the state to assume risk, including any corporation, association, partnership, nonprofit hospital, medical or health care service organization, health maintenance organization, reciprocal exchange, inter insurer, Lloyd's insurer, fraternal benefit society, or multiple-employer welfare arrangement;
- (2) A self-funded plan subject to state regulation.
- (3) A preferred provider organization administrator.
- (4) "Insurer" does not include producers, insurance support organizations, foreign-domiciled risk retention groups, or foreign-domiciled reinsurers.

X. "Investigative consumer report" means a consumer report or portion of a consumer report in which information about an individual's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with the individual's neighbors, friends, associates, acquaintances, or others who may have knowledge concerning such items of information.

Commented [KJ15]: Definition from Model 670

Y. "Joint marketing agreement" means a written contract between a licensee and one or more financial institutions to market the licensee's own products or services or for the licensee and one or more financial institutions jointly to offer, endorse, or sponsor a financial product or service.

Z. "Licensee" means any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this state or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction. "Licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only regarding the excess lines placements placed pursuant to Section [insert section] of the state's laws.

Commented [KJ16]: This definition was taken from Model 668 but is very similar to the definition in Model 672

AA. "Non-admitted insurer" means an insurer that has not been granted a certificate of authority or is not otherwise authorized by the commissioner to transact the business of insurance in this state.

Commented [KJ17]: Model 672

Commented [KJ18]: Definition from Model 670-added "or is not otherwise authorized"

**Drafting Note:** Each state must make sure this definition is consistent with its surplus lines laws.

BB. "Nonaffiliated third party" means:

- (1) Any person except:
  - (a) An affiliate of a licensee; or
  - (b) A person employed jointly by a licensee and any company that is not an affiliate of the licensee; however, a nonaffiliated third party includes the other company that jointly employs the person.
- (2) Nonaffiliated third party includes any person that is an affiliate solely by virtue of the direct or indirect ownership or control of the person by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).



Version 1.2

CC. "Person" means any individual, corporation, association, partnership, or other legal entity.

DD. "Personal information" means any individually identifiable information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to a consumer that is by or on behalf of a licensee and is:

Commented [KJ19]: From Model 670

(1) Any of the following:

(a) Account balance information and payment history;

Commented [KJ20]: The information in F(1) (b)-(g) was taken directly from Model 672

(b) The fact that an individual is or has been one of the licensee's customers or has obtained an insurance product or service from the licensee;

(c) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer, unless such disclosure is required by federal or state law;

(d) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(e) Any information the licensee collects through an information-collecting device from a web server, such as internet cookies, if such information can reasonably identify or link back to an individual;

(f) Information from a consumer report;

(g) Information that would enable judgments, directly or indirectly, to be made about a consumer's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics;

Commented [KJ21]: The provision in F.(1)(h) was taken from Model 670

(h) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personal information that is not publicly available.

(i) "Sensitive personal information";

(j) "Health information;"

(k) Consumers' demographic data, in any form or medium that can reasonably be used to identify an individual; or

(l) Collections or sets of individually identifiable information pertaining to more than one consumer.

(2) "Personal information" does not include "de-identified information" or "aggregate consumer information."

EE. "Precise geolocation" means any data that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,750 feet.

FF. "Privileged information" means any personal information that:

Commented [KJ22]: Model 670

(1) Relates to a claim for insurance benefits or a civil or criminal proceeding involving a consumer; and

Version 1.2

- (2) Is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving a consumer.

**Drafting Note:** The phrase "in reasonable anticipation of a claim" contemplates that the insurer has actual knowledge of a loss but has not received formal notice of the claim.

- GG. "Process" or "processing" means any operation or set of operations performed by a licensee, whether by manual or automated means, on the personal information of any consumer, including the collection, use, sharing, storage, disclosure, analysis, deletion, retention, or modification of personal information.
- HH. "Producer" means [refer here to every appropriate statutory category of producer, including brokers, required to be licensed to do business in the state].

**Drafting Note:** This is necessary because many states have various terms for producers, or for producers of certain types of insurers.]

- II. "Publicly available" means any information about a consumer that a licensee has a reasonable basis to believe is lawfully made available from:
- (1) Federal, state, or local government records;
  - (2) Widely distributed media; or
  - (3) Disclosures to the general public that are required to be made by federal, state or local law.

**Commented [KJ23]:** This definition comes from the IDSA (Model 668) and Model 672

**Drafting Note:** Examples of "a reasonable basis" are: (1) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded; or (2) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number online or the consumer has informed you that the telephone number is not unlisted.

**Commented [KJ24]:** Examples take from Modell 672

- JJ. "Research activities" means systemic investigation, including development, testing, and evaluation, designed to develop or contribute to generalizable knowledge where there is sharing of personal information with nonaffiliated third parties. "Research activities" does not mean any of the following exempt research activities that are considered part of an insurance transaction:
- (1) Relating to rating or risk management;
  - (2) For actuarial studies;
  - (3) For internal (i) analytics or (ii) customer experience purposes;
  - (4) For product development;
  - (5) To an insurance support organization; or
  - (6) Subject to a research university Internal Review Board or Privacy Board approval which requires use of a process which follows confidentiality best practices and where a contract agreeing to such protection has been executed.

- KK. "Residual market mechanism" means an association, organization or other entity defined or described in Sections(s) [insert those sections of the state insurance code authorizing the establishment of a FAIR Plan, assigned risk plan, reinsurance facility, joint underwriting association, etc.]

**Commented [KJ25]:** Model 670 language

Version 1.2

**Drafting Note:** Those states having a reinsurance facility may want to exclude it from this definition if the state's policy is not to disclose to insureds the fact that they have been reinsured in the facility.

- LL. "Retain" "retention" or "retaining" means storing or archiving personal information that is in the continuous possession, use, or control of licensee or a third-party service provider.
- MM. "Sell" or "selling" means the exchange of personal information to a third party for monetary or other valuable consideration.
- NN. "Sensitive personal information" means personal information including a consumer's (i) social security, driver's license, state identification card, or passport number; (ii) account log-in or financial account, debit card, or credit card numbers in combination with any required security or access code, password, or credentials allowing access to an account; (iii) precise geolocations; (iv) racial or ethnic origin, religious, or philosophical beliefs; (v) union membership; (vi) personal mail, personal email, and personal text messages content, unless the person in possession is the intended recipient of the communication; (vii) genetic information; (viii) a consumer's sex life or sexual orientation; (ix) citizenship or immigration status; (x) health information; or (xi) biometric information.

**Drafting Note:** Those states that have enacted a consumer data protection act may want to amend this definition to match that of the state's law.

- OO. "Share," "shared," or "sharing" means (i) disclosing, (ii) disseminating, (iii) making available, (iv) releasing, (v) renting, (vi) transferring, (vii) selling, or (viii) otherwise communicating by any means, a consumer's personal information whether or not for monetary or other valuable consideration, for providing insurance transactions or additional activities for the benefit of any party.
- PP. "Termination of insurance coverage" or "termination of an insurance policy" means either a cancellation or nonrenewal of an insurance policy, in whole or in part, for any reason other than failing to pay a premium as required by the policy.
- QQ. "Third-party service provider" means a person that contracts with a licensee that provides services to the licensee, and processes, shares, or otherwise is permitted access to personal information through its provisions of services to the licensee. "Third-party service provider" also includes a person with whom a licensee does not have a continuing business relationship and does not have a contract but may have to share personal or publicly available information in connection with an insurance transaction. Third-party service providers do not include (i) government entities; (ii) licensees; (iii) affiliates of licensees; and (iv) financial entities with whom licensees have joint marketing agreements.
- RR. "Value-added service or benefit" means a product or service that:
  - (1) Relates to insurance coverage applied for or purchased by a consumer; and
  - (2) Is primarily designed to satisfy one or more of the following:
    - (a) Provide loss mitigation or loss control services or products designed to mitigate risks related to the insurance requested by or offered to a consumer;
    - (b) Reduce claim costs or claim settlement costs;
    - (c) Provide education about liability risks or risk of loss to persons or property;



Commented [KJ26]: Model 670

Commented [KJ27]: From Model 668 but modified for this model

Commented [KJ28]: This definition was taken primarily from Model 880 (rebating)

Version 1.2

- (d) Monitor or assess risk, identify sources of risk, or develop strategies for eliminating or reducing risk;
- (e) Enhance the health of the consumer, including care coordination;
- (f) Enhance financial wellness of the consumer through education or financial planning services;
- (g) Provide post-loss services;
- (h) Incentivize behavioral changes to improve the health or reduce the risk of death or disability of a customer (defined for purposes of this subsection as policyholder, potential policyholder, certificate holder, potential certificate holder, insured, potential insured or applicant); or
- (i) Assist in the administration of employee or retiree benefit insurance coverage.

**Drafting Note:** Examples of “value-added services and benefits” are services or benefits related to (i) health and wellness, (ii) telematic monitoring, or (iii) property replacement services.

- SS. “Verifiable request” means a request that the licensee can reasonably verify, using commercially reasonable methods, is made by the consumer whose personal information is the subject of the request.
- TT. “Written consent” means any method of capturing a consumer’s consent that is capable of being recorded or maintained for as long as the licensee or third-party service provider has a business relationship with a consumer; or the licensee or third-party service provider is required to maintain the information as provided in this Act.

**ARTICLE II. OBLIGATIONS HANDLING CONSUMER’S PERSONAL INFORMATION**

**Section 3. Oversight of Third-Party Service Provider Arrangements**

- A. A licensee shall exercise due diligence in selecting its third-party service providers.
- B. No licensee shall (i) engage a third-party service provider to collect, process, or retain, or share any consumer’s personal information, or (ii) share any consumer’s personal information with any third-party service provider for any purpose unless there is a written contract between the licensee and third-party service provider that requires the third-party service provider to abide by the provisions of this Act and the licensee’s own privacy protection practices in the collection, processing, retention, or sharing of any consumer’s personal information.
- C. Notwithstanding Subsection 3B, a licensee may share a consumer’s publicly available information with a third-party service provider with whom the licensee has no written contract in connection with a claim only to the extent necessary to provide the service requested by the consumer.
- D. A licensee shall require all the licensee’s third-party service providers to implement appropriate measures to comply with the provisions of this Act in relation to consumers’ personal information that is collected, processed, or retained by, or shared with or otherwise made available to the third-party service providers in connection with (i) any insurance transactions or (ii) any additional activities.
- E. No licensee shall permit the third-party service provider to collect, process, retain, or share any consumer’s personal information in any manner:
  - (1) Not permitted by this Act; and

Version 1.2

(2) Not consistent with the licensee's own privacy protection practices.

F. A contract between a licensee and third-party service provider shall require that no third-party service provider shall further share or process a consumer's personal information other than as specified in the contract with the licensee.

G. Contracts between a licensee and any third-party service providers shall require either entity to honor the consumer's directive, whether it is an opt-in or an opt-out, and to refrain from collecting, processing, retaining, or sharing the consumer's personal information in a manner inconsistent with the directive of the consumer.

**Section 4. Data Minimization**

A. No licensee shall collect, process, retain, or share a consumer's personal information unless:

(1) The collection, processing, retention, or sharing is in compliance with this Act;

(2) The licensee provides the applicable notices required by this Act;

(3) The collection, processing, retention, or sharing of the consumer's personal information is consistent with and complies with the most recent privacy protection practices notice provided to the consumer by the licensee; and

(4) The collection, processing, retention, or sharing of the consumer's personal information is reasonably necessary and proportionate to achieve the purposes related to the requested insurance transaction or additional activities and not further processed, retained, or shared in a manner that is incompatible with those purposes;

B. No licensee shall permit any of its officers, employees, or agents to collect, process, retain, or share any consumer's personal information, except as relevant and necessary as part of that person's assigned duties.

**Section 5. Sharing Limitations**

A. Consistent with the requirements of this Act, a licensee may collect, process, retain, or share a consumer's personal information in connection with an insurance transaction as necessary:

(1) For the servicing of any insurance application, policy, contract, or certificate for a consumer, third-party claimant, or beneficiary;

(2) For compliance with a legal obligation to which the licensee is subject;

(3) For compliance with a request or directive from a law enforcement or insurance regulatory authority;

(4) For compliance with a warrant, subpoena, discovery request, judicial order, or other administrative, criminal, or civil legal process, or any other legal requirement that is binding upon the licensee collecting, processing, retaining, or sharing the personal information;

(5) For a lienholder, mortgagee, assignee, lessor, or other person shown on the records of an insurer or producer as having a legal or beneficial interest in a policy of insurance, to protect that interest provided that:

(a) No health information is shared unless the sharing would otherwise be permitted by this section, and

**Commented [KJ29]:** Most of these requirements were taken from Model 670 Section 13 and Model 672

Version 1.2

- (b) The information shared is limited to that which is reasonably necessary to permit such person to protect its interests in such policy;
- (6) To enable a licensee to detect or prevent criminal activity, fraud, material misrepresentation, or material nondisclosure in connection with an insurance transaction;
- (7) To enable a health care provider to:
  - (a) Verify the consumer's insurance coverage or benefits;
  - (b) Inform a consumer of health information of which the consumer may not be aware; or
  - (c) Conduct an operations or services audit to verify the individuals treated by the health care provider; provided only such information is shared as is reasonably necessary to accomplish the audit;
- (8) To permit a party or a representative of a party to a proposed or consummated sale, transfer, merger or consolidation of all or part of the business of the licensee to review the information necessary for such transaction, provided:
  - (a) Prior to the consummation of the sale, transfer, merger, or consolidation only such information is shared as is reasonably necessary to enable the recipient to make business decisions about the purchase, transfer, merger, or consolidation; and
  - (b) The recipient agrees not to share the acquired personal information until the recipient has complied with the provisions of this Act;
- (9) For an affiliate whose only use of the information is to perform an audit of a licensee provided the affiliate agrees not to process personal information for any other purpose or to share the personal information.
- (10) To permit a group policyholder to report claims experience or conduct an audit of the operations or services of a licensee, provided the information shared is reasonably necessary for the group policyholder to make the report or conduct the audit and is not otherwise shared;
- (11) To permit (i) a professional peer review organization to review the service or conduct of a healthcare provider provided the personal information is not otherwise processed or shared or (ii) to permit arbitration entities to conduct an arbitration related to a consumer's claim;
- (12) To provide information to a consumer regarding the status of an insurance transaction;
- (13) To permit a governmental authority to determine the consumer's eligibility for health care benefits for which the governmental authority may be liable;
- (14) Pursuant to a joint marketing agreement, provided a licensee shall not, directly or through an affiliate, share a consumer's personal or publicly available information with any nonaffiliated third party for marketing to the consumer unless.
  - (a) The consumer is first provided a clear and conspicuous means to opt-out of such sharing;
  - (b) The consumer has been given a reasonable time to opt-out of the sharing; and

Commented [KJ30]: More restrictive than Model 670


Version 1.2

- (c) The authorization complies with Section 6 of this Act.
- (15) For the purpose of marketing an insurance or financial product or service, provided the consumer has been given the opportunity to opt-out of such marketing as follows:
  - (a) The consumer is first provided a clear and conspicuous means to opt-out of such sharing;
  - (b) The consumer has been given a reasonable time to opt-out of the sharing; and
  - (c) The authorization complies with Section 6 of this Act.
- B. No licensee shall share any health information or privileged information about a consumer with a nonaffiliated third-party:
  - (1) Without first providing the consumer a clear and conspicuous notice that such information will not be shared unless the consumer opts-in to such sharing;
  - (2) The consumer has been given a reasonable time to opt-in to the sharing; and
  - (3) The authorization complies with Section 6 of this Act.
- C. No licensee may collect, process, or share a consumer's personal information in connection with any additional activities without first providing the consumer a clear and conspicuous notice that such information will not be collected, processed, or shared unless the consumer opts-in to such collection and use of personal information. Once consent has been obtained, any person may conduct additional activities as follows:
  - (1) For non-exempt research activities:
    - (a) No consumer may be identified in any research study or report;
    - (b) All materials allowing the consumer to be identified are returned to the licensee that initiated the activity; and
    - (c) A consumer's personal information is deleted as soon as the information is no longer needed for the specific activity.
  - (2) For all additional activities:
    - (a) The person conducting the activity agrees not to further share any consumer's personal information and only use such information for the purposes for which it was shared; and
    - (b) A consumer's sensitive personal information may not be shared or otherwise provided to any person for use in connection with any additional activity involving marketing a non-insurance or non-financial product or service.
- D. A licensee may collect, process, retain, or share consumers' de-identified personal information as necessary in connection with insurance transactions and additional activities.
- E. Notwithstanding any other provision of law, no licensee or its third-party service providers may sell consumers' personal information for any type of consideration. This subsection does not prohibit the following activities unless the licensee or third-party service provider receives money or marketable property in connection with these activities:

Version 1.2

- (1) The disclosure is to a third party for the purpose of or in support of providing an insurance or financial product or service requested by the consumer.
- (2) A licensee provides or receives information to an insurance support organization, statistical agent, or reinsurer;
- (3) A licensee provides information to an affiliate or to a financial institution with which the licensee performs joint marketing;
- (4) The business transfers to a third party the personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's assets; or
- (5) A consumer uses or directs the licensee to (i) disclose personal information; or (ii) interact with one or more licensees or other financial institutions.

F. This section shall not prohibit the collection, processing, retention, or sharing of consumers' personal information with a licensee's affiliates to the extent preempted by subdivisions (b)(1)(H) or (b)(2) of Section 625 of the Fair Credit Reporting Act.

**Section 6. Consumers' Consent** 

A. Where the consumer's consent for the collection, processing, or sharing of a consumer's personal or privileged information by a licensee is required by this Act, whether opt-in or opt-out, a licensee shall provide a reasonable means to obtain written consent and maintain a written record of such consent.

- (1) No licensee shall collect, process, or share personal information in a manner inconsistent with the choices of a consumer pursuant to this Act.
- (2) A licensee may provide the consent form together with or on the same written or electronic form as the most recent of the initial or updated notice the licensee provides or in a separate communication with the consumer.
- (2) If two (2) or more consumers jointly obtain an insurance or financial product or service from a licensee, the licensee may provide a single consent notice. Each of the joint consumers may consent or refuse to consent.
- (3) A licensee does not provide a reasonable means of obtaining express written consent if consent is required or the consumer is instructed that consent is required.
- (4) A licensee shall comply with a consumer's consent choice as soon as reasonably practicable after the licensee receives it.
- (5) Any consumer who has given consent for the collection, processing, and sharing of personal information in connection with additional activities, may revoke such consent in writing. A consumer may exercise the right to consent or to withdraw consent at any time with notice to the licensee.
- (6)
  - (a) A consumer's consent choice under this Act is effective until the consumer revokes it in writing.
  - (b) If the consumer subsequently establishes a new relationship with the licensee, the consent choices that applied to the former relationship do not apply to the new



## Version 1.2

relationship. A new relationship occurs when the consumer who previously ended all business relationships with the licensee re-establishes a business relationship more than thirty (30) days after the previous business relationship ended.

- (7) If the consumer has made conflicting choices pursuant to this section, the consumer's most recent written choice for the specific transaction or activity shall take precedence.
- B. When a consumer's consent is required, no person shall use an authorization seeking a consumer's consent, whether opt-out or opt-in, to the collection, processing, or sharing of a consumer's personal or privileged information unless the authorization meets following requirements.
- (1) Is written in plain language;
  - (2) Is dated and contains an expiration date for the consent;
  - (3) Specifies the persons authorized to collect, process, or share the consumer's personal or privileged information consistent with the provisions of this Act;
  - (4) Specifies the types of personal or privileged information authorized to be collected, processed, or shared;
  - (5) Specifies the specific purposes for which the consumer's personal or privileged information is authorized to be collected, processed, or shared as permitted in Article II of this Act;
  - (6) Names the licensee whom the consumer is authorizing to collect, process, or share the consumer's personal or privileged information; and
  - (7) Advises the consumer that they are entitled to receive a copy of the authorization.
- C. When requesting a consumer's consent to the collection, processing, or sharing of the consumer's personal information for additional activities, the written authorization shall;
- (1) Explain, in plain language, that consent is being sought to share the consumer's personal information for research activities by a person other than the licensee, or if the personal information is to be used for an additional activity, clearly explain the nature of that activity;
  - (2) Permit the consumer to separately provide consent for such use of the consumer's personal information for any one or more additional activities;
  - (3) Explain, in plain language, that the consumer is not required to provide consent to use the consumer's personal information for any one or all these purposes, and that the consumer will not be subject to retaliation or discrimination as outlined in Section 15, based on the consumer's choice; and
  - (4) State that use of a consumer's sensitive personal information for marketing purposes is prohibited.
  - (5) The provisions of Subsection B of this section do not apply to consumers' personal or privileged information that has been de-identified in accordance with this Act.

### **Section 7. Retention and Deletion of Consumers' Information**

- A. Once the initial consumer privacy protection practices notice has been provided to the consumer as set forth in this Act, a licensee may retain a consumer's personal or publicly information as necessary for:

Version 1.2


- (1) Performance of any insurance transaction with a consumer who is in an ongoing business relationship with the licensee;
  - (2) Compliance with a legal obligation related to any insurance transaction or any additional activity involving consumers' personal information to which the licensee is subject including but not limited to any state, federal, or international statute of limitation periods applicable to the licensee in connection with consumers' personal information;
  - (3) Compliance with a request or directive from a law enforcement agency or state, federal, or international regulatory authorities a warrant, subpoena, discovery request, judicial order, or other administrative, criminal, or civil legal process, or another legal requirement that is binding upon a licensee;
  - (4) Protection of a legal or beneficial interest in a policy of insurance, with respect to a lienholder, mortgagee, assignee, lessor, or other person shown on the records of an insurer or producer as having a legal or beneficial interest in the policy; or
  - (5) Exempt research activities (i) related to insurance transactions involving consumers' personal information, or (ii) for rating or risk management purposes for or on behalf of the licensee in connection with an insurance product or service.
- B. Not less than annually, a licensee shall review its retention policy and all consumers' personal information in its possession and determine whether the purposes for which such personal information was collected or processed remain.
- C. Once the provisions of Subsection A of this section are no longer applicable and the licensee has made the determination that consumers' personal information is no longer needed under Subsection B of this section:
- (1) Such licensee shall completely delete all the consumer's personal information within 90 days after making this determination.
  - (2) Subject to the approval of the commissioner, any licensee that retains consumers' personal information on a system or systems where targeted disposal is not feasible, shall de-identify all such information to the extent possible.
    - (a) If such information cannot be de-identified or deleted, the licensee shall:
      - (i) Develop a written data minimization plan that provides for transitioning from such system or systems within a reasonable time frame and the projected date for such transition; and
      - (ii) Annually, report in detail the licensee's progress for such transition to its domestic regulator who shall determine the reasonableness of such plan and whether the licensee is making the appropriate progress in implementing such plan.
    - (b) A licensee has made a reasonable effort to transition from legacy systems if the licensee's transition plan is designed to be completed within 10 years after the effective date of the Act.
  - (3) The commissioner has discretion to grant exceptions for good cause shown.
  - (4) Any third-party service provider in possession of the consumer's personal information shall delete such information at the earlier of:

Version 1.2

- (a) The date the contract the licensee has with the third-party service provider ends;  
or
  - (b) The date specified in such contract.
- (5) If a consumer requests a copy of the consumer's personal information that has been deleted or de-identified as provided in this Act, the licensee shall inform the consumer that the licensee and any of the licensee's third-party service providers in possession of the consumer's personal information no longer retain any of the consumer's personal information or such information has been de-identified;
- (6) A licensee shall develop policies and procedures for compliance with this section and be able to demonstrate compliance with those policies and procedures.

**ARTICLE III. NOTICES AND DELIVERY OF NOTICES**

**Section 8. Notice of Consumer Privacy Protection Practices**

- A. A licensee that collects, processes, retains, or shares a consumer's personal or publicly available information in connection with an insurance transaction, by whatever means used, shall provide the consumer a clear and conspicuous notices that accurately reflect the licensee's privacy protection practices. The following exceptions apply to this requirement:
- (1) No notice of privacy protection practices is required of a reinsurer or in connection with the provision of reinsurance.
  - (2) An employee, agent, representative or designee of a licensee, who is also a licensee, is not required to develop or provide a notice of consumer privacy protection practices to the extent that the collection, processing, retention, and sharing of personal information by the employee, agent, representative or designee of such licensee is consistent with the consumer privacy protection practices of such licensee and the licensee provides the notice required in this section.
  - (3) A licensee that does not share and does not wish to reserve the right to share, personal information of consumers except (i) in connection with an insurance transaction or (ii) as authorized under Section 5 may satisfy the notice requirements under this section by providing the initial privacy protection practices notice as set forth in Subsection 8B.
- B. (1) A licensee shall provide an initial notice of privacy protection practices to a consumer at the time the licensee, directly or through a third-party service provider, first collects, processes, or shares the consumer's personal or publicly available information in connection with an insurance transaction or additional activity. For purposes of this subsection, consumer includes a third-party claimant or a beneficiary in connection with a claim under an insurance policy.
- (2) For any consumer with whom a licensee has an ongoing business relationship and whose personal or publicly available information has been collected, processed, retained, or shared prior to the effective date of this Act in this State, a notice meeting the requirements of this Act must be provided upon renewal or any reinstatement of the consumer's policy, or upon any other activity related to an insurance transaction if the consumer has not already been provided a notice meeting the requirements of this Act.
- C. A licensee shall provide an updated privacy protection practices notice to each consumer with whom the licensee has an ongoing business relationship when the privacy protection practices of the licensee changes. 

Version 1.2

- (1) The licensee shall conspicuously identify any changes in its privacy protection practices that triggered the requirement for an updated notice.
  - (2) An updated notice shall also be provided to any third-party claimant or beneficiary if there are changes in the licensee's privacy protection practices during the course of any claim in which such claimant or beneficiary is involved.
- D. Each version of a licensee's privacy protection practices notice shall contain an effective date that must remain on the notice until the licensee revises the notice due to a change in its privacy protection practices. The licensee shall place a revised date on its updated notice that will remain until the notice is revised in response to additional changes in the licensee's privacy protection practices.
- E. A licensee shall honor all representations made to consumers in its most current notice, unless otherwise compelled by law, in which case the licensee shall promptly send a notice to all affected consumers explaining the changes in the licensee's information practices. If the licensee's information practices change, the licensee remains bound by the terms of the most recent notice it has given a consumer, until a revised notice has been given.

**Section 9. Content of Consumer Privacy Protection Practices Notices**

- A. Any notice required by Section 8 of this Act shall state in writing all the following:
- (1) Whether personal information has been or may be collected from any sources other than the consumer or consumers proposed for coverage, and whether such information is collected by the licensee or by third-party service providers;
  - (2) The categories of consumer's personal information that the licensee or any of its third-party service providers has or may collect, process, retain, or share;
  - (3) The purposes for which the licensee collects, processes, retains, or shares personal information;
  - (4) The sources that have been used or may be used by the licensee to collect, process, retain, or share the consumer's personal information;
  - (5) That the consumer may, upon request, annually obtain a list of any persons with which the licensee or any of the licensee's third-party service providers has shared the consumer's personal information within the current calendar year and, at a minimum, the three previous calendar years.
  - (6) A description of the right to opt-out of sharing of personal information for marketing or an insurance or financial product or service, including marketing pursuant to a joint marketing agreement;
  - (7) A description of the requirements set forth in Section 5C if the licensee shares a consumer's personal information in connection with additional activities including:
    - (a) The requirement that the licensee obtain the consumer's express written consent for the collection, processing, retention, or sharing of a consumer's personal information for research activities not conducted by or on behalf of the licensee unless such information has been de-identified;
    - (b) The requirement for the licensee to obtain the consumer's express written consent for the collection, processing, retention, or sharing of a consumer's personal information for marketing a non-insurance or non-financial product or service.

**Commented [KJ31]:** This is language is consistent with Model 910 (Record Retention)

Version 1.2

- (c) The requirement that the licensee obtain the consumer's express written consent for the collection, processing, retention, or sharing of a consumer's personal information for any other additional activity; and
  - (d) A description of the process by which a consumer may opt-out of such collection, processing, or sharing.
  - (8) A statement of the rights of the consumer to access, correct or amend factually incorrect personal publicly available information about the consumer in the possession of the licensee or its third-party service providers under Article IV of this Act, and the instructions for exercising such rights;
  - (9) A statement of the rights of non-retaliation established under Section 15 of this Act;
  - (10) A summary of the reasons the licensee or any third-party service provider retains personal information and the approximate period of retention or if that is not reasonably possible, the criteria used to determine the timeframe it will be retained; and
  - (11) A statement that no licensee or third-party service provider may sell for valuable consideration a consumer's personal information.
  - (12) If the licensee or its third-party service providers processes or shares personal, privileged, or publicly available information with an entity located outside the jurisdiction of the United States and its territories, the notice must state that such information is processed or shared in this manner. This requirement does not apply if the only processing or sharing is:
    - (a) In connection with a reinsurance transaction; or
    - (b) With an affiliate of the licensee.
- B. If the licensee uses a consumer's personal information to engage in additional activities, in addition to the provisions in Subsection A of this section, the following information shall be included in the notice:
- (1) A statement that the consumer may, but is not required to, consent to the collection, processing, sharing, and retention of the consumer's personal information for any additional activities in which the licensee or its third-party service providers engage;
  - (2) A description of the reasonable means by which the consumer may express written consent;
  - (3) That the consumer may consent to any one or more of the additional activities or refuse to consent to any one or more of the additional activities;
  - (4) That once consent has been given for an additional activity, the consumer may revoke consent at any time;
  - (5) That once consent for using a consumer's personal information for an additional activity is withdrawn, the licensee will no longer engage in such additional activity using the consumer's personal information; and
  - (6) That once consent to an additional activity has been revoked, any of the consumer's personal information in the possession of the licensee used solely for that additional activity will be destroyed and deleted as set forth in Section 6 of this Act.

Version 1.2

- C. The obligations imposed by this section upon a licensee may be satisfied by another licensee or third-party service provider authorized to act on its behalf.

**Section 10. Notice of Consumer Privacy Rights**

- A. A licensee shall provide a Notice of Consumer Privacy Rights to each consumer with whom the licensee has an ongoing business relationship.
- B. The notice required by this section shall be clear and conspicuous and inform the consumer that:
  - (a) The consumer has the right to access personal information about the consumer;
  - (b) The consumer has the right to correct or amend inaccurate or incomplete information about the consumer;
  - (c) The consumer has the right to opt-out of use of personal information for additional activities;
  - (d) The consumer must opt-in to use of sensitive personal information for additional activities;
  - (e) The consumer has the right to request additional information about the licensee's privacy practices, including identification of all persons who have received the consumer's personal information within the last three years;
  - (f) A licensee may not retaliate against a consumer, or require a consumer to incur unreasonable expenses, in connection with exercise of rights under this Act.
- C. The notice required by this section shall be provided to the consumer at least every 12 months.
- D. The notice required by this section shall be in addition to other notices required by this Act.
- E. The notice required by this section may be combined with other policy documents, provided that the notice content required by this section remains clear and conspicuous and is readily distinguishable from other information being provided to the consumer.

**Section 11. Delivery of Notices Required by This Act**

- A. A licensee shall provide any notices required by this Act so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically pursuant to [State's UETA law].
- B. A licensee may reasonably expect that a consumer will receive actual notice if the licensee:
  - (1) Hand-delivers a printed copy of the notice to the consumer;
  - (2) Mails a printed copy of the notice to the address of record of the consumer separately, or in a policy, billing, or other written communication;
  - (3) For a consumer who has agreed to conduct transactions electronically, either (i) posts the notice on the licensee's website and requires the consumer to acknowledge receipt of the notice or (ii) emails the notice to the consumer and requests a delivery receipt.
- C. A licensee may not reasonably expect that a consumer will receive actual notice of its privacy protection practices if it:

Commented [KJ32]: This language comes from Model 672

Version 1.2

- (1) Only posts a sign in its office or generally publishes advertisements of its privacy protections practices; or
  - (2) Sends the notice electronically to a consumer who has not agreed to conduct business electronically with the licensee.
  - (3) Sends the notice electronically to a consumer who has agreed to conduct business electronically with the licensee, but the licensee does not obtain a delivery receipt.
  - (4) Provides a notice required by this Act solely by orally explaining the notice, either in person or over the telephone or other electronic device unless the licensee also sends a copy of the notice to the consumer.
  - (5) Does not provide the notices required by this Act so that the consumer is able to retain them or obtain them later in writing; either electronically or on paper.
- D. A licensee may reasonably expect that a consumer will receive actual notice of the licensee's privacy protection practices notice if:
- (1) If the consumer has agreed to conduct business electronically pursuant to the State's UETA and:
    - (a) The consumer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or
    - (b) The licensee emails the notice to the consumer's email address of record.
  - (2) The licensee mails the notice to the consumer's address of record.
  - (3) A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or using an electronic means unless specifically requested to do so by the consumer.
  - (4) The licensee provides all notices required by this Act so that the consumer can retain and obtain the notices in writing.
- E. A licensee may provide a joint notice from the licensee and one or more of its affiliates if the notice accurately reflects the licensee's and the affiliate's privacy protection practices with respect to the consumer.
- F. If two (2) or more consumers jointly obtain a product or service in connection with an insurance transaction from a licensee, the licensee may satisfy the initial and updated notice requirements of Sections 8 and 9 of this Act, by providing one notice to those consumers jointly. The notice must reflect the consent of each consumer.
- G. If any consumer has requested that the licensee refrain from sending updated notices of privacy protection practices and the licensee's current privacy protection practices notice remains available to the consumer upon request, the licensee shall honor the consumer's request but must continue to send any jointly insured consumer any updated notices.
- H. In addition to the notice provided to consumers, a licensee shall prominently post and make available the notice required by this Act on its website, if a website is maintained by the licensee. The licensee shall design its website notice so that:

Commented [KJ33]: This language is from Model 672

Version 1.2

- (a) The notice is clear and conspicuous;
- (b) The text or visual cues encourage scrolling down the page, if necessary, to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and
- (c) The notice is:
  - (i) Placed on a screen that consumers frequently access, such as a page on which transactions are conducted; or
  - (ii) Accessible using a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature, and relevance of the notice.

**ARTICLE IV. CONSUMERS' RIGHTS**



**Section 12. Access to Personal and Publicly Available Information**

- A. Any consumer may submit a verifiable request to a licensee for access to the consumer's personal and publicly available information in the possession of the licensee or its third-party service providers.
- B. The licensee or third-party service provider shall
  - (1) Acknowledge the request within five (5) business days; and
  - (2) Within forty-five (45) business days from the date such request is received:
    - (a) Disclose to the consumer the identity of those persons to whom the licensee or any third-party service provider has shared the consumer's personal information within the current year and, at a minimum, the three calendar years prior to the date the consumer's request is received.
    - (b) Provide the consumer with a summary of the consumer's personal information and the process for the consumer to request a copy of such information in the possession of the licensee.
    - (c) Identify the source of any consumer's personal information provided to the consumer pursuant to this subsection.
- C. Personal health information in the possession of licensee and requested under Subsection A of this section, together with the identity of the source of such information, shall be supplied either directly to the consumer or as designated by the consumer, to a health care provider who is licensed to provide medical care with respect to the condition to which the information relates. If the consumer elects for the licensee to disclose the information to a health care provider designated by the consumer, the licensee shall notify the consumer, at the time of the disclosure, that it has provided the information to the designated health care provider.
- D. The obligations imposed by this section upon a licensee may be satisfied by another licensee authorized to act on its behalf.
- E. The rights granted to consumers in this section shall extend to any individual to the extent personal information about the individual is collected processed, retained, or shared by a licensee or its third-party service provider in connection with an insurance transaction or an additional activity.



Commented [KJ34]: From Model 910





Version 1.2

- F. For purposes of this section, the term “third-party service provider” does not include “consumer reporting agency” except to the extent this section imposes more stringent requirements on a consumer reporting agency than other state or federal laws.
- G. The rights granted to any consumer by this subsection shall not extend to information about the consumer that is collected, processed, retained, or shared in connection with, or in reasonable anticipation of, a claim, or civil or criminal proceeding involving the consumer.

**Section 13. Correction or Amendment of Personal or Publicly Available Information**


- A. Any consumer may submit a verifiable request to a licensee to correct or amend any personal or publicly available information about the consumer in the possession of the licensee or its third-party service providers.
- B. The licensee or third-party service provider shall
  - (1) Acknowledge the request within five (5) business days; and
  - (2) Within fifteen (15) business days from the date such request is received:
    - (a) Correct or amend the personal or publicly available information in dispute; or
    - (b) If there is a specific legal basis for not correcting or amending the personal or publicly available information in question, the licensee or its third-party service provider may refuse to make such correction or amendment. However, the licensee or third-party service provider refusing to take such action shall provide the following information to the consumer:
      - (i) Written notice of the refusal to make such correction or amendment;
      - (ii) The basis for the refusal to correct or amend the information;
      - (iii) The contact information for filing a complaint with the consumer’s state insurance regulator, and
      - (iv) The consumer’s right to file a written statement as provided in Subsection C of this section.
  - (3) No licensee or third-party service provider may refuse to correct or amend a consumer’s personal or publicly available information without good cause. Such cause shall be demonstrated to commissioner of the consumer’s state insurance department, upon request.

C. If the licensee or third-party service provider corrects or amends personal publicly available information in accordance with Subsection A. (1) of this section, the licensee or third-party service provider shall so notify the consumer in writing and furnish the correction or amendment to:

- (1) Any person specifically designated by the consumer who may have, received such personal or publicly available information within the preceding two (2) years;
- (2) Any insurance support organization whose primary source of personal information is insurers if the insurance support organization has systematically received such personal information from the insurer within the preceding five (5) years; provided, however, that the correction or amendment need not be furnished if the insurance support organization no longer maintains personal information about the consumer;

Commented [KJ35]: This section is from Model 670 with a shortening of the length of time for B 2

Version 1.2

- (3) Any third-party service provider that furnished such personal or publicly available information.
- D. Whenever a consumer disagrees with the refusal of a licensee or third-party service provider to correct or amend personal or publicly available information, the consumer shall be permitted to file with the licensee or third-party service provider a concise statement setting forth 
  - (1) The relevant and factual information that demonstrates the errors in the information held by the licensee or third-party service provider; and
  - (2) The reasons why the consumer disagrees with the refusal of the licensee or third-party service provider to correct or amend the personal or publicly available information.
- E. In the event a consumer files such statement described in Subsection C, the licensee or third-party service provider shall:
  - (1) Include the statement with the disputed personal or publicly available information and provide a copy of the consumer's statement to anyone reviewing the disputed personal or publicly available information; and
  - (2) In any subsequent disclosure of the personal or publicly available information that is the subject of disagreement, the licensee or third-party service provider clearly identify the matter or matters in dispute and include the consumer's statement with the personal or publicly available information being disclosed.
- F. The rights granted to a consumer by this subsection shall not extend to personal or publicly available information about the consumer that is collected, processed, retained, or shared in connection with or in reasonable anticipation of a claim, or civil or criminal proceeding involving the consumer.
- G. For purposes of this section, the term "insurance support organization" does not include "consumer reporting agency" except to the extent that this section imposes more stringent requirements on a consumer reporting agency than other state or federal law.

**Section 14. Adverse Underwriting Decisions**

- A. In the event of an adverse underwriting decision the licensee responsible for the decision shall:
  - (1) Either provide in writing to the consumer at the consumer's address of record:
    - (a) The specific reason or reasons for the adverse underwriting decision, or
    - (b) That upon written request the consumer may receive the specific reason or reasons for the adverse underwriting decision in writing; and
  - (2) Provide the consumer with a summary of the rights established under Subsection C of this Section and Sections 12 and 13 of this Act.

**Drafting Note:** Adverse underwriting decisions include: (i) an increase in the risk; (ii) increase in rates in geographical area; (iii) increase base rates; (iv) change in insurance credit score that causes an increase in the premium; (v) the consumer has lost a discount; (vi) an insured had a claim; or (vii) a lapse in coverage.

- B. Upon receipt of a written request within ninety (90) business days from the date of a notice of an adverse underwriting decision was sent to a consumer's address of record, the licensee within fifteen (15) business days from the date of receipt of such request shall furnish to the consumer the following information in writing to the consumer's address of record:

**Commented [KJ36]:** The provisions in this section are largely from Model 670 with some amendments

Version 1.2

- (1) The specific reason or reasons for the adverse insurance decision, if such information was not initially furnished pursuant to Subsection A(1);
- (2) The specific information that supports those reasons, provided;
  - (a) A licensee shall not be required to furnish specific privileged information if it has a reasonable suspicion, based upon specific information available for review by the commissioner, that the consumer has engaged in criminal activity, fraud, material misrepresentation or material nondisclosure, or
  - (b) Health information supplied by a health care provider shall be disclosed either directly to the consumer about whom the information relates or to a health care provider designated by the individual consumer and licensed to provide health care with respect to the condition to which the information relates,
- (3) A summary of the rights established under Subsection C and Sections 12 and 13 of this Act; and

**Drafting Note:** The exception in Section 14 B(2)(a) to the obligation of an insurance institution or agent to furnish the specific items of personal or privileged information that support the reasons for an adverse underwriting decision extends only to information about criminal activity, fraud, material misrepresentation or material nondisclosure that is privileged information and not to all information.

- (4) The names and addresses of the sources that supplied the information outlined in Subsection B(2); provided, however, that the identity of any health care provider shall be disclosed either directly to the consumer or to the health care provider designated by the consumer.
- C. No licensee may base an adverse underwriting decision:
- (1) Solely on the loss history of the previous owner of the property to be insured.
  - (2) Personal information obtained from a third-party service provider whose primary unless further supporting information is provided to the licensee.
  - (3) Any previous adverse underwriting decision received by the consumer unless such inquiries also request the reasons for any previous adverse underwriting decision.
- D. The obligations imposed by this section upon a licensee may be satisfied by another licensee authorized to act on its behalf.

**Section 15 Nondiscrimination and Nonretaliation**

- A. A licensee and third-party service providers shall not retaliate against a consumer because the consumer exercised any of the rights under this Act. There shall be a rebuttable presumption that a licensee or third-party service provider has discriminated or retaliated against a consumer if:
- (1) The consumer is required to consent to an additional activity to obtain a particular product, coverage, rate, or service;
  - (2) The consumer is required to consent to an additional activity to obtain an insurance transaction;
  - (3) The licensee or third-party service provider charges a consumer who makes an annual request for access to the consumer's personal or publicly available information pursuant to Section 12 of this Act;

Version 1.2

- (4) The licensee or third-party service provider charges a consumer who requests the consumer's personal or publicly available information be amended or corrected pursuant to Section 13 of this Act; or
- (5) The licensee or third-party service provider crates unreasonable barriers to a consumer's exercise of the rights provided in Sections 12 and 13 of this Act.

**Drafting Note:** This section incorporates similar provisions from Model 672.

- B. There shall be a rebuttable presumption that consistent with a licensee's filed rules, rates, and forms, and normal underwriting guidelines in the State in which the consumer resides, the following acts do not constitute discrimination or retaliation if the act is reasonably related to any change in price or quality of services or goods applicable to all customers if the licensee is an insurer or a producer, or if a third-party service provider on behalf of a licensee:
  - (1) Charges a different rate or premium to the consumer;
  - (2) Provides a different insurance product,
  - (3) Refuses to write insurance coverage for the consumer; or
  - (4) Denies a claim under an insurance product purchased by the consumer.

**ARTICLE VI. ADDITIONAL PROVISIONS**

**Section 16. Investigative Consumer Reports**

- A. No licensee may prepare or request an investigative consumer report about a consumer in connection with an insurance transaction involving an application for insurance, a policy renewal, a policy reinstatement, or a change in insurance benefits unless the licensee informs the consumer in writing prior to the report being prepared that the consumer:
  - (1) May request to be interviewed in connection with the preparation of the investigative consumer report and the licensee shall conduct such interview; and
  - (2) Is entitled to receive a written copy of the investigative consumer report.
- B. If a licensee uses a third-party service provider to obtain an investigative consumer report, the written contract between the licensee and the third-party service provider shall require the third-party service provider to:
  - (1) Comply with the requirements of Subsection 18 A;
  - (2) Not otherwise use any personal information provided to the third-party service provider by the licensee or obtained by the third-party service provider in its investigation of the consumer other than to fulfill the purpose of the contract with the licensee.
- C. If a licensee requests a third-party service provider to prepare an investigative consumer report, the licensee requesting such report shall notify in writing the third-party service provider whether a personal interview has been requested by the consumer. The third-party service provider shall conduct the interview requested.
- D. A licensee that prepares or requests an investigative consumer report in connection with an insurance claim shall notify the consumer that the consumer may request to be interviewed in connection with the preparation of the investigative consumer report. However, neither the licensee

Version 1.2

nor the third-party service provider is required to provide a copy of an investigative report prepared in connection with an insurance claim unless compelled to do so by a state or federal court.

**Section 17. Compliance with HIPAA and HITECH**

- A. A licensee that is subject to and compliant with the privacy and notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and collects, processes, retains, and shares all personal information in the same manner as protected health information shall be deemed to be in compliance with this Act.
- B. Any such licensee shall submit to the [commissioner] a written statement from an officer of the licensee certifying that the licensee collects, processes, retains, and shares all personal information in the same manner as protected health information.
- C. Any such licensee that does not fully comply with Sections 17 A and B shall be subject to all provisions of this Act with respect to personal information.

**ARTICLE VII GENERAL PROVISIONS**

**Section 18. Power of Commissioner**

- A. The commissioner 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 Act. [This power is in addition to the powers which the commissioner has under [insert applicable statutes governing the investigation or examination of insurers]. Any such investigation or examination shall be conducted pursuant to [insert applicable statutes governing the investigation or examination of insurers].
- B. The commissioner shall have the power to examine and investigate the affairs of any insurance support organization acting on behalf of a licensee that either transacts business in this state or transacts business outside this state that affects a person residing in this state to determine whether such insurance support organization has been or is engaged in any conduct in violation of this Act.

**Drafting Note:** Section 18 B is optional. The drafters included this language for those states that had already adopted Model 670 and those states that wish to adopt this provision.

- C. Whenever the commissioner has reason to believe that a licensee has been or is engaged in conduct in this State which violates this Act, the commissioner may take action that is necessary or appropriate to enforce the provisions of this Act.

**Section 19. Confidentiality**

- A. Any documents, materials, data, or information in the control or possession of the state insurance department that are furnished by a licensee, third-party service provider, or an employee or agent thereof, acting on behalf of the licensee pursuant to this Act, or that are obtained by the commissioner in any investigation, or an examination pursuant to Section 19 of this Act shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the commissioner is authorized to use the documents, materials, or other information in the furtherance of any regulatory or legal action brought as a part of the commissioner's duties.

**Commented [KJ37]:** This provision is consistent with Model 668

**Commented [KJ38]:** This language comes from Model 670

**Commented [KJ39]:** This language comes from Model 668.

**Commented [KJ40]:** This language was taken from Model 668 and modified for the purposes of this model.

Version 1.2

- B. Neither the commissioner nor any person who receives documents, data, materials, or information while acting under the authority of the commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 20 A.
- C. In order to assist in the performance of the commissioner's duties under this Act, the commissioner:
- (1) May share documents, data, materials or information, including the confidential and privileged documents, data, materials, or information subject to Section 20 A, with other state, federal, and international regulatory agencies, with the National Association of Insurance commissioners, its affiliates or subsidiaries, any third-party consultant or vendor, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the documents, data, materials, or information; and
  - (2) May receive documents, data, materials, or information, including otherwise confidential and privileged documents, data, materials, or information, from the National Association of Insurance commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any documents, data, materials, or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the documents, data, materials, or information.
  - (3) Shall enter into a written agreement with any third-party consultant or vendor governing sharing and use of documents, data, materials, or information provided pursuant to this Act, consistent with this subsection that shall:
    - (a) Specify that the third- party consultant or vendor agrees in writing to maintain the confidentiality and privileged status of the documents, data, materials, or information subject to Section 20 A;
    - (b) Specify that the ownership of the documents, data, materials, or information shared pursuant to Section 20 A with the third-party consultant or vendor remains with the commissioner, and the third-party consultant's or vendor's use of the information is subject to the direction of, the commissioner;
    - (c) Prohibit the third-party consultant or vendor from retaining the documents, data, materials, or information shared pursuant to this Act after the purposes of the contract have been satisfied; and
    - (d) Require prompt notice be given to the commissioner if any confidential documents, data, materials, or information in possession of the third-party consultant or vendor pursuant to this Act is subject to a request or subpoena to the third-party consultant or vendor for disclosure or production.
- E. No waiver of any applicable privilege or claim of confidentiality in the documents, data, materials, or information shall occur due to disclosure to the commissioner under this section or due to sharing as authorized in-Section 20 C.
- F. Nothing in this Act shall prohibit the commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or subsidiaries.

Version 1.2

**Section 20. Record Retention**

- A. Notwithstanding any other provision of law, a licensee shall maintain sufficient evidence in its records of compliance with this Act for the calendar year in which the activities governed by this Act occurred and the three calendar years thereafter.
- B. A licensee or third-party service provider shall maintain all records necessary for compliance with the requirements of this Act, including, but not limited to:
- (1) Records related to the consumer's right of access pursuant to Article IV;
  - (2) Copies of authorizations and consent\ executed by any consumer pursuant to this Act, for as long as the consumer is in a continuing business relationship with the licensee; and
  - (3) Representative samples of any notice required to be provided to any consumer pursuant to this Act, for as long as the consumer is in a continuing business relationship with the licensee.

Commented [KJ41]: Language from Model 910

**Section 21. Hearings, Records, and Service of Process**

Whenever the commissioner has reason to believe that a licensee or its third-party service providers have been or are engaged in conduct in this state which violates this Act,[ or if the commissioner believes that a third-party service provider has been or is engaged in conduct outside this state that affects a person residing in this state and that violates this Act], the commissioner shall issue and serve upon such a licensee or its third-party service provider a statement of charges and notice of hearing to be held at a time and place fixed in the notice. The date for such hearing shall be not less than [insert number] days after the date of service.

- A. At the time and place fixed for such hearing a licensee or its third-party service provider[, or third-party service provider] charged shall have an opportunity to answer the charges against it and present evidence on its behalf. Upon good cause shown, the commissioner shall permit any adversely affected person to intervene, appear and be heard at such hearing by counsel or in person.
- B. At any hearing conducted pursuant to this section the commissioner may administer oaths, examine, and cross-examine witnesses and receive oral and documentary evidence. The commissioner shall have the power to subpoena witnesses, compel their attendance and require the production of books, papers, records, correspondence and other documents, and data that are relevant to the hearing. A record of the hearing shall be made upon the request of any party or at the discretion of the commissioner. If no record is made and if judicial review is sought, the commissioner shall prepare a statement of the evidence for use on the review. Hearings conducted under this section shall be governed by the same rules of evidence and procedure applicable to administrative proceedings conducted under the laws of this state.
- C. Statements of charges, notices, orders, and other processes of the commissioner under this Act may be served by anyone duly authorized to act on behalf of the commissioner. Service of process may be completed in the manner provided by law for service of process in civil actions or by registered or certified mail. A copy of the statement of charges, notice, order, or other process shall be provided to the person or persons whose rights under this Act have been allegedly violated. A verified return setting forth the manner of service or return receipt in the case of registered or certified mail, shall be sufficient proof of service.

**Drafting Note:** Consideration should be given to the practice and procedure in each state.

**Section 22. Service of Process -Third-Party Service Providers**

For purposes of this Act, a third-party service provider transacting business outside this state that affects a person residing in this state shall be deemed to have appointed the commissioner to accept service of process on its behalf;

Version 1.2

provided the commissioner causes a copy of such service to be mailed forthwith by registered or certified mail to the third-party service provider at its last known principal place of business. The return receipt for such mailing shall be sufficient proof that the same was properly mailed by the commissioner.

**Section 23. Cease and Desist Orders and Reports**

- A. If, after a hearing pursuant to Section 22, the commissioner determines that licensee or its third-party service provider charged has engaged in conduct or practices in violation of this Act, the commissioner shall reduce his or her findings to writing and shall issue and cause to be served upon such licensee or its third-party service provider a copy of such findings and an order requiring such licensee or its third-party service provider to cease and desist from the conduct or practices constituting a violation of this Act.
- B. If, after a hearing, the commissioner determines that the licensee or its third-party service provider charged has not engaged in conduct or practices in violation of this Act, the commissioner shall prepare a written report which sets forth findings of fact and conclusions of law. Such report shall be served upon the insurer, producer, or insurance support organization charged and upon the person or persons, if any, whose rights under this Act were allegedly violated.
- C. Until the expiration of the time allowed for filing a petition for review or until such petition is filed, whichever occurs first, the commissioner may modify or set aside any order or report issued under this section. After the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed, the commissioner may, after notice and opportunity for hearing, alter, modify, or set aside, in whole or in part, any order or report issued under this section whenever conditions of fact or law warrant such action or if the public interest so requires.

**Drafting Note:** Consideration should be given to the practice and procedure in each state.

**Section 24. Penalties**

In the case of a violation of this Act, a Licensee may be penalized in accordance with [insert general penalty statute].

**Drafting Note:** Consideration should be given to the practice and procedure requirements and penalty requirements in each state.

**Section 25. Judicial Review of Orders and Reports**

- A. Any person subject to an order of the commissioner under [Code cite] or any person whose rights under this Act were allegedly violated may obtain a review of any order or report of the commissioner by filing in the [insert title] Court of [insert county] County, within [insert number] days from the date of the service of such order or report, a written petition requesting that the order or report of the commissioner be set aside. A copy of such petition shall be simultaneously served upon the commissioner, who shall certify and file in such court the entire record of the proceeding giving rise to the order or report which is the subject of the petition. Upon filing of the petition and record the [insert title] Court shall have jurisdiction to make and enter a decree modifying, affirming, or reversing any order or report of the commissioner, in whole or in part. The findings of the commissioner as to the facts supporting any order or report, if supported by clear and convincing evidence, shall be conclusive.
- B. To the extent an order or report of the commissioner is affirmed, the Court shall issue its own order commanding obedience to the terms of the order or report of the commissioner. If any party affected by an order or report of the commissioner shall apply to the court for leave to produce additional evidence and shall show to the satisfaction of the court that such additional evidence is material and that there are reasonable grounds for the failure to produce such evidence in prior proceedings, the court may order such additional evidence to be taken before the commissioner in such manner and upon such terms and conditions as the court may deem proper. The commissioner may modify his



Version 1.2

or her findings of fact or make new findings by reason of the additional evidence so taken and shall file such modified or new findings along with any recommendation, if any, for the modification or revocation of a previous order or report. If supported by clear and convincing evidence, the modified or new findings shall be conclusive as to the matters contained therein.

- C. An order or report issued by the commissioner shall become final:
- (1) Upon the expiration of the time allowed for the filing of a petition for review, if no such petition has been duly filed; except that the commissioner may modify or set aside an order or report; or
  - (2) Upon a final decision of the [insert title] Court if the court directs that the order or report of the commissioner be affirmed or the petition for review dismissed.
- D. No order or report of the commissioner under this Act or order of a court to enforce the same shall in any way relieve or absolve any person affected by such order or report from any liability under any law of this state.

**Drafting Note:** Consideration should be given to the practice and procedure in each state.

**Section 26. Individual Remedies**

[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.

Commented [KJ42]: Language from Model #668

**Section 27. Immunity**

No cause of action in the nature of defamation, invasion of privacy or negligence shall arise against any person for disclosing personal or privileged information in accordance with this Act, nor shall such a cause of action arise against any person for furnishing personal or privileged information to an insurer, producer, or insurance support organization; provided, however, this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person.

**Section 89. Obtaining Information Under False Pretenses**

No person shall knowingly and willfully obtain information about a consumer from a licensee under false pretenses. A person found to be in violation of this section shall be fined not more than [insert dollar amount] or imprisoned for not more than [insert length of time], or both.

**Drafting Note:** This provision is applicable to states requiring this language.

**Section 29. Severability**

If any provisions of this Act or the application of the Act to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected.

**Section 30. Conflict with Other Laws**

- A. All laws and parts of laws of this state inconsistent with this Act are hereby superseded with respect to matters covered by this Act.
- B. Nothing in this article shall preempt or supersede existing federal or state law related to protected health information.

Version 1.2

**Section 32. Rules and Regulations**

The commissioner may issue such rules, regulations, and orders as shall be necessary to carry out the provisions of this Act.

**Section 33. Effective Date and Compliance Dates**

- A. This Act shall take effect on [insert a date].
- B. Licensees shall have ## years from the effective date of this Act to implement Section ## of this Act.
- C. Licensees shall have ## years from the effective date of this Act to implement Section ## of this Act.

July 26, 2023

**Via Email**

Ms. Katie Johnson  
Virginia Bureau of Insurance  
Chair, NAIC Privacy Protections (H) Working Group (PPWG)

Re: Revised Exposure Draft of the Insurance Consumer Privacy Protection Model Law (the "ICPP Model") Issued July 11, 2023 (the "July Exposure Draft")

Dear Ms. Johnson:

This comment letter is submitted on behalf of Underwriters at Lloyd's, London ("Lloyd's") in response to the July Exposure Draft. The Lloyd's market is the largest writer of surplus lines insurance in the United States writing business in all 50 states via the 81 syndicates that appear on the Quarterly Listing of Alien Insurers maintained by the International Insurers Department of the NAIC. Lloyd's appreciates the huge amount of work the PPWG has done in its efforts to develop a privacy framework for the insurance sector. However, at the outset we must note disappointment with the accelerated process and timing for consideration of the July Exposure Draft. We appreciate that the PPWG provided significant time for public comment and feedback on the first draft. However, given the breadth of the subject matter the ICPP Model is attempting to address, it must be expected that multiple drafts and minimum 30-day comment periods will be needed in order for all drafting issues to be properly considered and addressed. Endeavoring to meet an artificial deadline for completion of this project will result in a flawed work product which is not fit for purpose. We urge the PPWG to adjust its workplan expectations to allow for a full and transparent public comment process as has always been standard procedure in regard to the drafting of NAIC Model Laws.

**Licensee Definition & Treatment of the Surplus Lines Market**

As Lloyd's noted in our March comment letter, the ICPP Model deviates from the typical definition of "licensee" used in most NAIC models by adding an additional sentence which incorporates unauthorized insurers into the definition of licensee. As we explain further below, Lloyd's believes that the inclusion of unauthorized insurers in the definition of licensee creates fundamental problems in regard to how the ICPP Model will apply in the surplus lines market. We note that historically unauthorized insurers have not been considered licensees because the licensee in a surplus lines transaction is the surplus lines broker which must be licensed in the home state of the transaction.

Lloyd's has no objection to privacy regulation – we comply with GDPR in our home jurisdiction of the UK – however, if the ICPP Model is to be applied to the surplus lines market it must be done in a way that recognizes the differences in the way surplus lines business is placed and regulated as compared with the admitted market.

The surplus lines market provides coverage for complex risks and is an important source of capacity in US geographies that have significant exposure to natural disasters. It is a secondary market to be accessed when coverage cannot be purchased in the admitted market. As a result, consumers do not deal directly with surplus lines insurers. Rather it is surplus lines brokers that gather the information needed to determine the right placement option for a consumer. With this background of how surplus lines transactions are conducted in mind, Lloyd's suggests that unauthorized insurers should be removed from the definition of licensee. A surplus lines insurer that obtains consumer personal information from a surplus lines broker would then be considered a third party service provider under the ICPP Model. This is appropriate since surplus lines insurers only obtain consumer information through the brokers that place business with them who are themselves licensees under the ICPP Model.

### **Insurer Definition**

We believe it is the intention of the PPWG to exclude reinsurance from the ICPP Model. This is logical since the purpose of the ICPP Model is to protect consumer information and reinsurance transactions do not involve such information. However, the definition of insurer as currently drafted excludes only "foreign-domiciled reinsurers." Lloyd's recommends that the definition of insurer in Section 2(W)(4) be revised to also exclude "alien-domiciled reinsurers" to make clear that reinsurers domiciled outside the United States are not subject to the insurer definition, just as is the case with foreign reinsurers, i.e. US reinsurers domiciled outside the adopting state.

### **Adverse Underwriting Decision**

Lloyd's respectfully suggested that the inclusion of Section 14 Adverse Underwriting Decisions in a Model designed and intended to address privacy of consumer information is inappropriate. Consumer privacy is a broad and complex topic as the PPWG knows. It is not practical to attempt to cover another topic as challenging and detailed as providing transparency in underwriting decisions within the same Model Law and during the same drafting and comment process. These topics both deserve the full attention and careful consideration of interested parties. Yet it is clear that Section 14 has received little attention thus far. To be clear, Lloyd's believes that Section 14 should be removed from the ICPP Model. We reiterate below comments we made in our March comment letter to highlight the problems that exist with Section 14 as currently drafted.

As previously mentioned, the ICPP Model deviates from the typical NAIC definition of a licensee by including unauthorized insurers, also known as nonadmitted insurers, in the definition of licensee. At the same time, the definition of "adverse underwriting decision" in Section (B)(1)(d)(i) says that an adverse underwriting decision includes, "Placement by an insurer or producer of a risk with a...non-admitted insurer, or an insurer that specializes in substandard risks." In this framework, with unauthorized/nonadmitted insurers both a licensee and within the adverse underwriting regime, if a state were to adopt Section 14, then surplus lines carriers, such as Lloyd's, would be obligated to notify their clients that by virtue of having Lloyd's coverage they have been subject to an adverse underwriting decision. This would be a perverse and punitive requirement, which is not supported in fact. Additionally, nonadmitted insurers are already required to provide notices that highlight for consumers the differences between admitted and nonadmitted coverage.

The obvious way to fix this problem is to remove unauthorized/nonadmitted insurers from the definition of licensee. However, even if this change is made, Lloyd's believes the PPWG must reconsider the proposed definition of "adverse underwriting decision" as it does not reflect the commercial realities of insurance markets in certain geographies within the US. Lloyd's rejects the suggestion that coverage provided by a nonadmitted insurer is in any way "adverse." Indeed, many consumers, regulators, and

legislators would also not consider coverage with a nonadmitted insurer to be ~~adverse, harmful, or a~~ negative outcome. Securing coverage from a nonadmitted insurer is often the difference between a consumer either going without coverage entirely or procuring coverage from a state-backed residual market. In areas subject to hurricanes and wildfires, nonadmitted insurers, such as Lloyd's, provide an important source of capacity where admitted markets have pulled back. These nonadmitted carriers are providing a valuable service by providing insurance where others will not, and in so doing are helping to close the protection gap – something the NAIC has spent years trying to achieve and is one of its 2023 objectives. These nonadmitted insurers should not at the same time be subject to the pejorative label of an “adverse underwriting decision.”

Lloyd's appreciates the opportunity to offer these comments and would be glad to discuss them further with the Working Group.

Very truly yours,



Sabrina Miesowitz  
General Counsel



Timothy W. Grant  
Associate General Counsel

616 Fifth Avenue, Suite 106  
Belmar, NJ 07719  
732-201-4133  
CHIEF EXECUTIVE OFFICER: Thomas B. Considine



Attachment 3 - NCOIL Comments  
Privacy Protections Working Group  
8/13/23

**PRESIDENT:** Rep. Deborah Ferguson, AR  
**VICE PRESIDENT:** Rep. Tom Oliverson, TX  
**TREASURER:** Asw. Pamela Hunter, NY  
**SECRETARY:** Sen. Paul Utke, MN

**IMMEDIATE PAST PRESIDENTS:**  
Rep. Matt Lehman, IN  
Sen. Travis Holdman, IN

July 27, 2023

Katie Johnson  
Chair, Privacy Protections (H) Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106-2197

*Attn: Lois Alexander, NAIC Market Regulation Manager*  
*Via e-mail: [lalexander@naic.org](mailto:lalexander@naic.org)*

**RE: NCOIL Comments on Draft Insurance Consumer Privacy Protection Model Law (#674)**

Dear Chair Johnson:

Thank you for the opportunity to provide comments on the latest draft of the Insurance Consumer Privacy Protection Model Law (Model). The National Council of Insurance Legislators (NCOIL) values its longstanding relationship with the National Association of Insurance Commissioners (NAIC), and we look forward to working with you and the Working Group on this very important issue.

We acknowledge that comments on the Model are due by July 28. However, we have just recently concluded our Summer National Meeting last week in Minneapolis, and we have not had time to review the Model and draft specific comments. Accordingly, please accept this letter as meeting the July 28 deadline, and we will follow up with specific comments in August.

With appreciation for your consideration and best regards, I am,

Very truly yours,

A handwritten signature in blue ink that reads "Tom Considine".

Thomas B. Considine  
CEO  
NCOIL



/NCOILorg

**WEBSITE:** [www.ncoil.org](http://www.ncoil.org)



/NCOILorg

***Sound Public Policy In 50 States For 50-Plus Years***



July 27, 2023

Katie Johnson, Chair  
Privacy Protections (H) Working Group  
National Association of Insurance Commissioners  
c/o Ms. Lois Alexander  
Manager – Market Regulation  
Via email [lalexander@naic.org](mailto:lalexander@naic.org)

**Re: RAA Comments Regarding Exposure Draft of New *Consumer Privacy Protections Model Law #674***

Dear Ms. Johnson:

The Reinsurance Association of America (RAA) appreciates the opportunity to submit comments to the Privacy Protections (H) Working Group regarding the most recent exposure draft of the *Consumer Privacy Protections Model Law (#674)*. The Reinsurance Association of America (RAA) is a national trade association representing reinsurance companies doing business in the United States. RAA membership is diverse, including reinsurance underwriters and intermediaries licensed in the U.S. and those that conduct business on a cross-border basis. The RAA also has life reinsurance affiliates and insurance-linked securities (ILS) fund managers and market participants that are engaged in the assumption of property/casualty risks. The RAA represents its members before state, federal and international bodies.

The RAA appreciates the Working Group’s continued thoughtful engagement to update the model act. The RAA is pleased the Working Group has moved to address some of the concerns raised by the RAA with the prior exposure draft but some concerns have yet to be addressed. The RAA also continues to support the concerns raised in our letter dated April 3, 2023 and by our primary insurance colleagues and, rather than reiterating those comments, will focus our comments on reinsurance specific issues at this time. The RAA supports and appreciates the changes in the updated exposure draft to exempt reinsurers from notice requirements and remove the restriction on sharing data across international borders, although some slight clarification on the notice section may still be needed.

The RAA has one primary reinsurance-related concern remaining with the current draft: the continuing lack of clarity as to whether and the extent to which reinsurers would fall within the definitions of “insurers”, “licensees”, and/or “third-party service providers”, which creates confusion as to how the law would apply to reinsurers and what their obligations would be under it.

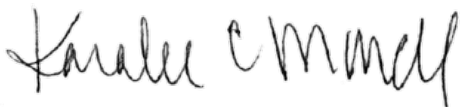
Reinsurance Association of America  
Page 2

As drafted, the definitions treat reinsurers inconsistently, including potential different treatment of foreign-domiciled reinsurers and domestic reinsurers. For example, under the definition of “insurer”, reinsurers seem to be included under subsection (1), but subsection (4) exempts foreign-domiciled reinsurers. The definition of “licensee” seems to similarly exclude only assuming insurers domiciled in another state or jurisdiction. Lastly, even if reinsurers are not considered insurers or licensees, the broad definition of “third-party service provider” including “any person that obtains consumers’ personal information from a licensee” could be read to include any reinsurer not falling within the definitions of insurer or licensee. The definitions require revision with respect to scope and application to reinsurers. The RAA is also concerned that the current definitions would put entities like (re)insurance brokers, considered both a “licensee” and “third-party service provider”, at a double disadvantage for consent requirements, given the nature of their business and interactions with insurance companies. This is in contrast to all other key privacy laws which recognize different obligations for primary businesses than for service providers. The RAA believes that a new definition defining reinsurers and/or reinsurance may be needed to address this issue.

The RAA is still in the process of receiving feedback from its members on this issue and plans to submit additional follow-up comments and suggested redline changes prior to the Summer National Meeting in Seattle. These brief initial comments serve only to continue to highlight the remaining concerns the RAA has for the Working Group.

The RAA understands the efforts to amend this model will be ongoing for quite some time. The RAA appreciates the opportunity to work with you on this important project and specifically to address the reinsurance-specific concerns. We would be happy to meet with members of the Privacy Protections (H) Working Group and NAIC staff to discuss reinsurance operations and the regulation of reinsurance under state law. We look forward to further engagement on these issues.

Sincerely,



Karalee C. Morell  
SVP and General Counsel  
Reinsurance Association of America



July 27, 2023

Ms. Katie Johnson  
Virginia State Corporation Commission/Bureau of Insurance  
Chair, NAIC Privacy Protections Working Group  
NAIC Central Office  
1100 Walnut Street, Suite 1500  
Kansas City, MO. 64106

*Attn: Ms. Lois Alexander, NAIC Market Regulation Manager*  
*Sent via email: lalaalexander@naic.org*

**Re: Comments on Sections 13 and 20 of the NAIC Insurance Consumer Privacy Protection Model Law #674**

Dear Ms. Johnson:

We are writing on behalf of LexisNexis Risk Solutions Inc. (“LexisNexis”), a leader in providing essential information to help customers across industries and government assess, predict, and manage risk. LexisNexis appreciates the opportunity to provide feedback on the draft NAIC Insurance Consumer Privacy Protection Model Law #674 (“Model Law”).

LexisNexis is greatly appreciative of the continued comprehensive and inclusive stakeholder process the NAIC has undergone as it seeks to identify the best approach for the Model Law. The NAIC Privacy Protection Working Group (“NAIC”) continues to show its willingness to identify a privacy framework that is both operationally feasible for carriers and provides necessary protections for consumers. The comments below are intended to assist the NAIC in refining the most recent proposed draft provisions of Section 13 and Section 20.

\*\*\*

The FCRA, as well as NAIC Model 670 that exposed draft Model 674 pulls language from, provides for a 30-day response period regarding a request to a third-party service provider to correct or amend personal or publicly available information about a consumer. However, Model 674 Section 13.B.(1-2) requires a third-party service provider to acknowledge a request to correct or amend personal or publicly available information about a consumer within five business day and either correct or provide a response within fifteen days. Per 12 CFR Part 1022 The Fair Credit Reporting Act’s Limited Preemption of State Laws, the FCRA expressly preempts certain categories of State laws. As relevant here, 15 U.S.C. 1681t(b) says:

*No requirement or prohibition may be imposed under the laws of any State:*

- (1) with respect to any subject matter regulated under*
  - (A) subsection (c) or (e) of section 1681b of this title, relating to the prescreening of consumer reports;*
  - (B) section 1681i of this title, relating to the time by which a consumer reporting agency must take any action, including the provision of notification to a*

*consumer or other person, in any procedure related to the disputed accuracy of information in a consumer's file, except that this subparagraph shall not apply to any State law in effect on September 30, 1996.*

Additionally, reducing this time to fifteen days would be difficult for third-party service providers to achieve with the due diligence required of such a review, and could encourage fraudulent disputes as the significantly shortened timetable could lead to an increase in suppression of accurate data that service providers are unable to verify within fifteen days of the request.

Regarding Section 20.B(2-3), draft Model 674 requires that third-party service providers maintain 1) copies of “authorization and consent executed by any consumer pursuant to this Act, for as long as the consumer is in a continuing business relationship with the licensee” and 2) “representative samples of any notice required to be provided to any consumer pursuant to this act as long as the consumer is in a continuing business relationship with the licensee.” The model that this section borrows from, Model 910, has retention requirements of three years. Increasing this requirement to the length of the business relationship, which could greatly surpass the original three-year requirement, would generally conflict with the record retention policies of most companies.

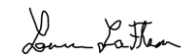
For the above reasons, we respectfully request the NAIC modify draft Model 674 to align with the current FCRA requirements to avoid preemption issues and limit document retention to the currently prescribed three-year limit in order to not cause confusion regarding the length of time documents must be maintained, promote consistency, and to not unduly burden companies that have longstanding relationships with insurers.

\*\*\*

Thank you for your consideration of these comments. To the extent they have not already, we fully anticipate that other industry participants will provide more detailed feedback and observations.

LexisNexis looks forward to future opportunities to comment on revised drafts of the Model Law. Should you have any questions, please do not hesitate to contact us at [Lauren.LaFleur@lexisnexisrisk.com](mailto:Lauren.LaFleur@lexisnexisrisk.com) or [Jon.Burton@relx.com](mailto:Jon.Burton@relx.com).

Sincerely,



Lauren LaFleur  
Corporate Counsel  
LexisNexis Risk Solutions Inc.



Jon Burton  
Managing Director, State Government Relations  
RELX, Inc.



July 28, 2023

Privacy Protections (H) Working Group  
National Association of Insurance Commissioners  
c/o Ms. Lois Alexander  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106  
Via email to [LAlexander@naic.org](mailto:LAlexander@naic.org)

RE: Privacy Protections Working Group Drafting Pod – Amended Provisions of Model #674

Dear Ms. Alexander:

I am writing on behalf of the National Insurance Crime Bureau (“NICB”) to address concerns with the National Association of Insurance Commissioners’ (NAIC) Privacy Protections Working Group (PPWG) Drafting Pod’s amended provisions of draft Model #674. This letter follows NICB’s April 3 and July 10 letters regarding draft Model #674.

NICB continues to have concerns with the revised draft Model #674 for the reasons stated in our previous letters. This past legislative session, seven additional states passed consumer data privacy laws that included entity-level exemptions for NICB. That brings the total number of states having enacted consumer data privacy statutes with specific NICB exemptions to ten. It would be inconsistent with those state laws for the NAIC model not to include a similar exemption in order to fight insurance crime and fraud, and for all the reasons stated in our letters.

We appreciate PPWG’s engagement with NICB to date and look forward to further discussions.

We appreciate your consideration of our concerns. If you have any questions or need additional information, please contact me at [rdizinno@nicb.org](mailto:rdizinno@nicb.org) or 703.216.0994.

Respectfully,

/s/ Richard E. DiZinno

Richard E. DiZinno  
Vice President  
Strategy, Policy and Government Affairs  
National Insurance Crime Bureau

**NAIC CONSUMER REPRESENTATIVE COMMENTS  
ON MODEL 674 VERSION 1.2**

To: Katie Johnson, Chair and Cynthia Amann, Co-Vice Chairs - Privacy Protections (H) Working Group

cc: Lois Alexander, Jennifer McAdam, NAIC Working Group Staff

Date: July 27, 2023

**Re: Model 674 Exposure Draft, Version 1.2**

---

We the undersigned NAIC Consumer Representatives applaud the efforts of the NAIC Privacy Protections (H) Working Group to increase the protection of consumers' personal information collected by insurers, other insurance licensees and their third-party service providers. We all agree that these changes are long overdue, given that the previous NAIC models protecting consumer information were written decades ago, when abuses of consumer information were much less common. We are pleased to see that the provisions in Model 674 will improve consumer protections. Below we cite areas where we feel the provisions in Version 1.2 should be improved or strengthened.

Data Minimization - Deletion of Data No Longer Needed

Section 4.B that states that no licensees should retain any consumer's personal information, "except as relevant and necessary as part of that person's assigned duties". Supporting that requirement, Section 7.C requires licensees to completely delete all consumer personal information no longer needed within 90 days after making that determination. However, that Section allows exceptions where a 90 day timeline is not deemed feasible. In such cases, Section 7.C(2)(b) states that 10 years is a reasonable transition period for legacy systems. Ten years is totally unreasonable, effectively giving licensees the ability to disregard the deletion requirement. If the Model is to prescribe a reasonable transition period for deletion in Section 7.C(2)(b), a shorter time, such as three years, should be required for legacy *and non-legacy* systems, unless the licensee can demonstrate a legitimate reason for further delay.

Deletion of similar information by third-party service providers (TPSP's) is just as important as deletion by licensees. Section 7.C(4) requires TPSP's to delete such data at the time their contract with a licensee ends or by a date specified in such a contract. That is totally unacceptable. Licensees should require their TPSP's to delete data within 90 days of notification. If that is not feasible, then licensees should seek exemptions from this requirement, just as they would under Section 7.C.

Regarding legacy information systems, we find it odd that industry representatives who said they could not *delete* unneeded data due to legacy systems, did not say they could not *correct* consumer information, which is required under the circumstances outlined in Section 13. If they have the ability to correct incorrect or outdated consumer information, they should be able to delete consumer information by replacing it with null data sets.

Finally, in situations where a licensee or TPSP is unable to delete data, Section 7 should require that they not use or share such data under any circumstance.

### Opt-In or Opt-Out Consents

A universal concern of consumers is that privacy requests for opt-ins or opt-outs are frequently too long to expect consumers to carefully read them and too generic in scope. In such cases, consent may be applied in situations, where they would not want to give it. Language should be added to Model 674 to require consent requests to be very specific regarding the information used, how it will be used, and how long it will be used.

The following sentences from the European Union GDPR illustrates the language needed:

"For marketing purposes, consent must be specific and based on appropriate information provided the individual. Blanket consent without specifying the exact purpose of use is not acceptable."

Regarding time limits for consents, Section 6.A(6)(a) states a consumer's consent is effective until the consumer revokes it in writing. This is contradicted by Section 6.B(2), which states that consents should be dated and have an expiration date. A specific expiration date should be required for all opt-in or opt-out consents that permit licensees and TPSP's to use or share information. In the real world, nearly all consumers will have forgotten consents they had even given in the past, and so it would not occur to them to revoke past consents. Section 6.A(6)(a) should be deleted.

### Consumer Information Categories in Consumer Privacy Protection Practice Notices

At the June in-person meeting of the Privacy Protections Working Group in Kansas City, there was a great deal of debate about what "categories" should be used in Privacy Protection Practice Notices to describe data that licensees and their TPSP's collect, process, retain, or share.

California's CCPA regulations establish the following 11 categories:

1. **Identifiers:** Name, alias, postal address, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers
2. **Customer records information:** Name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's

license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit or debit card number, other financial information, medical information, health insurance information

3. **Characteristics of protected classifications under California or federal law:** Race, religion, sexual orientation, gender identity, gender expression, age, disability
4. **Commercial information:** Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies
5. **Biometric information:** Hair color, eye color, fingerprints, height, retina scans, facial recognition, voice, and other biometric data
6. **Internet or other electronic network activity information:** Browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement
7. **Geolocation data**
8. **Audio, electronic, visual, thermal, olfactory, or similar information**
9. **Professional or employment-related information**
10. **Education information:** Information that is not "publicly available personally identifiable information" as defined in the California Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99)
11. **Inferences:** The law refers to inferences that could be used to create a consumer profile:
  - Preferences
  - Characteristics
  - Psychological trends
  - Predispositions
  - Behavior
  - Attitudes
  - Intelligence
  - Abilities
  - Aptitudes

We recommend that Section III.9 on the content of Consumer Privacy Protection Practice Notices use these categories to specify consumer information that may be collected or used, with explanations of how this information is collected.

### Sections 9 and 10 - Notices of Consumer Privacy Protection Practices and Privacy Rights

These two sections in Model 674 delineate the information that should be included in the Notices of Consumer Privacy Protection Practices and Notices of Consumer Privacy Rights. It is well-established that the wording of such notices varies greatly across companies, and some companies even intentionally use obtuse language or burdensome processes, as in the use of dark patterns. We recommend that Model 674 provide templates that licensees and TPSP's would be required to utilize in the notices they provide. Examples of this practice are the notice templates provided by the federal government to prescribe the content and format of certain communications between private Medicare health plans and their enrollees.

## Section 14 - Notice of Adverse Underwriting Decisions

In the event of an adverse underwriting decision, Section 14.A gives the licensee responsible for the decision the option to either send the reasons for the adverse decision or to require the consumer to send a written request to get those reasons. Licensees should not have that second option, and so Section 14.A(1)(b) should be eliminated. It just puts an unnecessary burden on the consumer, for no justifiable reason. The only exception to this requirement should be that reasons related to concerns about criminal activity, fraud, material misrepresentation or material nondisclosure would not need to be disclosed, as described in the Drafting Note to Section 14.A.

Section 14.C(2) has a wording problem. The words "whose primary" should be deleted.

## Section 26 - Individual Remedies

There was a great deal of debate on one of the Working Group calls about whether there should be a private right of action when licensees or TPSP's violate the requirements of this Model Act. The NAIC Consumer Representatives on that call all felt that optional language to that effect should be kept in the Model. Version 1.2 of the Model eliminated that language.

In the event the data was kept after the business relationship has ended and subsequently used without permission or lost, the consumer should have an explicit private right of action against the insurer for maintaining data after it was no longer needed, for failing to timely disclose the use or theft of the data. Model 674 has no meaningful or timely enforcement mechanism for data deletion, which makes a private cause of action essential.

In California, a private right of action is permitted in cases where there are major data breaches of consumer information related to serious misconduct or violations of the CCPA. Especially since the Privacy Protections Working Group has not included data security provisions in Model 674, we suggest it would be appropriate to adopt some version of the following sections of California Code would be appropriate.

### **1798.150. Personal Information Security Breaches**

(a)(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of

this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.

In conclusion, we the undersigned NAIC Consumer Representatives appreciate the hard and thoughtful work that has gone into the development of Model 674. We hope you will adopt the recommendations submitted here and look forward to working with the Privacy Protections (H) Working Group to bring this tremendous effort to completion this year.

Sincerely,

Amy Bach

Birny Birnbaum

Bonnie Burns

Brenda Cude

Lucy Culp

Deborah Darcy

Yosha Dotson

Eric Ellsworth

Erica Eversman

Kelly Headrick

Marguerite Herman

Kara Hinkley

Karrol Kitt

Kenneth Klein

Rachel Klein

Peter Kochenburger

Dorianne Mason

Carl Schmid

Matthew Smith

Harold Ting

Wayne Turner

Richard Weber

Silvia Yee





July 28, 2023

Katie Johnson, Chair  
Privacy Protections (H) Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106-2197

Attn: Lois Alexander, NAIC Market Regulation Manager  
Via email: [lalexander@naic.org](mailto:lalexander@naic.org)

**RE: ACLI Comments on Version 1.2 of the Draft Insurance Consumer Privacy Protection Model Law (#674)**

Dear Chair Johnson:

Thank you for the opportunity to provide comments on Version 1.2 of the Insurance Consumer Privacy Protection Model Law (Model #674). We appreciate the time, energy, and consideration undertaken by the Privacy Protections Working Group and the positive intentions expressed within the Cover Page. Your summary of changes appears to recognize the consumer benefits that flow from enabling GLBA's approach to information collection, use, and affiliate sharing while also acknowledging the need to supplement and modernize to meet today's data-driven world. While some of the Working Group's changes to the draft are consistent with this shared goal, others are not. The most workable approach to developing a modernized privacy framework is to identify and enhance gaps in the widely-adopted GLBA regulatory model. Focusing on the areas of current law that need to be improved is less disruptive to the very successful current insurance privacy regulatory scheme for consumers, regulators and industry. Taking a novel approach, as the current draft represents, would be extremely disruptive to all stakeholders and mark the insurance industry as an outlier. In order to not disadvantage insurers, the privacy model must also be harmonized with the state consumer privacy laws now adopted in 11 states.

As currently drafted, Model #674 remains unworkable, overly burdensome, and confusing for industry, regulators, and consumers alike. At a high level, the comments below are meant to highlight several provisions ACLI members continue to find troubling with Model #674. Key provisions of concern include joint marketing; marketing; retention and deletion of consumer information; definitions; access and correction; notice- timing, content, and delivery; nondiscrimination and nonretaliation; consent versus authorizations; reinsurance concerns; and group insurance concerns. We hope these comments provide some guidance on which provisions need to be discussed in more detail, as we foresee potentially negative consequences.

Concerns

ACLI members appreciate several changes made by the Working Group to draft Model #674. For instance, the removal of the prohibition on cross-border sharing of personal information was the correct decision. And the amendments to the private cause of action provisions are very welcome. The new Model Law will have a great

**American Council of Life Insurers** | 101 Constitution Ave, NW, Suite 700 | Washington, DC 20001-2133

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 percent of industry assets in the United States.

impact on consumers as well as insurance company operations, so we want to get it right. The open calls and the in-person drafting meeting in June demonstrated that robust stakeholder engagement leads to improved outcomes. We want to keep that momentum going, however, ACLI members are concerned with the amount of time and process remaining.

We continue to strive to be an active and valued contributor to the Model #674 drafting process. Recognizing the need to provide input on the Working Group's timeline, we are highlighting the provisions of Version 1.2 that are most concerning to our members. In order for us to give the most constructive feedback in the limited time that is available to us, it would be extremely helpful to have an explanation from the drafters as to why several of our previously submitted comments and concerns were not addressed in this latest draft, so that we can better understand the current language and perhaps offer more constructive solutions rather than repeating old requests. Many of our previous suggestions would resolve some of the issues we raise once again below.

While we appreciate that the Working Group is open to receiving comments at any time and understand the desire to move the process forward, the pressure to adhere to arbitrary deadlines and respond to the ever-changing draft language impacts our ability to constructively engage. We understand that consistent stakeholder engagement can feel laborious, in part because it requires Working Groups and Committees to give stakeholders sufficient time to distribute information, collect feedback, and compile it to share with regulators. Throughout the drafting process, ACLI has made a good faith effort to engage with the Working Group and provide thorough feedback, including redline edits, detailed explanations, and suggested alternative language. As you all know, this level of engagement requires a tremendous amount of time and energy from our members. We remain committed to a high level of engagement, but we must give this project the time it warrants to meet the ultimate objective- uniform state adoption.

### Joint Marketing

While the Working Group's cover letter clearly states an intent to permit joint marketing agreements, Section 5(A)(14) requires further discussion to clarify that intent. In addition, other provisions in Version 1.2 include new and additional restrictions on joint marketing between financial institutions, a legal construct authorized by the Gramm-Leach-Bliley Act (GLBA). As just one example of where the draft restricts joint marketing, the model would require insurers to send privacy notices at first collection of a consumer's information from a joint marketing partner financial institution. That may be required even if the insurer does not market or share the consumer's information. Not only does the change have no beneficial effect for consumers, but it in fact would detrimentally affect the ability of insurers to provide a broader portfolio of financial services. The additional restrictions on joint marketing in the current draft are not in line with GLBA requirements and would establish restrictions that conflict with other existing regulations applicable to financial institutions.

### Marketing

Given the very broad definition of sensitive personal information, it is concerning that a consumer's sensitive personal information cannot be shared or otherwise provided to any person for use in connection with any additional activity involving marketing a non-insurance or non-financial product or service. At a time when industry and regulators are focused on closing the coverage gap and building financial resilience, this may impact certain companies' efforts to reach more consumers, especially middle-market and underserved consumers.

### Retention and Deletion of Consumer Information

Although improvements were made, Section 7 still includes several obligations that ACLI members find troubling. For instance, the inclusion of an annual review of "all consumers' personal information" in a licensee's possession

is logistically infeasible. ACLI members are also concerned by the new unnecessary administrative obligations that would compel licensees to migrate data off legacy systems within ten years of the Model Act. This provision does not serve to benefit consumers and is unnecessarily costly and burdensome. While precise estimates are difficult, companies have shared that in some instances it could take decades to migrate multiple/complex systems and tens of millions of dollars to retire legacy systems. As previously mentioned, ACLI strongly recommends that the Working Group consider a “reasonable period of time,” rather than 90 days, as well as the adoption of a feasibility standard.

Insurers spend millions of dollars annually to maintain cybersecurity and comprehensive information security programs to appropriately safeguard the personal information entrusted to them. Many of the Working Group’s data privacy and security concerns are already addressed under the NAIC Insurance Data Security Law (Model #668), the GLBA Safeguards Rule as adopted by states, and other regulatory frameworks to which insurers are subject. Given the longevity of a relationship with its customers (in some cases close to 100 years), many legacy systems that hold customer data are not designed to be able to do individualized consumer deletion, as with backup or WORM retention systems. Current laws have provided for a risk-based approach, understanding these systems have in place appropriate security controls and requests for these deletions for customer data are few. State insurance commissioners, after understanding current technical environments of insurers, should be provided discretion as to appropriate retention control standards.

### Definitions

Several key definitions remain concerning, with many of those concerns being interrelated with the other concepts raised in this letter. Below we highlight a few definitions that need to be discussed in more detail, as we foresee potentially negative consequences. This list is not all encompassing, and additional issues impacting definitions will need to be discussed.

The undefined term “*additional activities*” which has been inserted into Version 1.2 and placed throughout the latest draft Model #674 is problematic. This is an undefined term and would require consent and further limitations to collect, process, retain, or share consumer personal information.

The definition of “*sensitive personal information*” is still overly broad. As written, a consumer’s sensitive personal information cannot be shared or otherwise provided to any person for use in connection with any additional activity involving marketing a non-insurance or non-financial product or service. A consumer should have the right to consent to this sharing.

The definition of “*insurance transaction*” still needs further discussion, especially given the overall inclusion of transactions and services noted, as well as sections (7) and (8), which appear to be a drafting error.

The definition of “*nonaffiliated third-party*” does not expressly exclude service providers and/or insurance support organizations. This is important in particular because Section 5(B) prohibits sharing health information and privileged information about a consumer with a nonaffiliated third-party unless a consumer opts-in. Life insurers need to share that information with service providers in order to make underwriting decisions (e.g., sharing with a service provider to send paramedical providers for underwriting medical examinations), service claims or provide other services to in-force policy holders (e.g., sharing with a service provider to do an assessment of health status under a long-term care or disability insurance policy).

The term “*publicly available*” information appears to be added throughout the draft. This is especially concerning given the inconsistency with other laws and regulations and the inability for insurers to carry out the requirements noted in the draft rule.

The definition of “*consumer*” is extremely broad and should align with the definition in Model #672.

Similarly, the definition of “*personal information*” is broad given the extensive language detailing “any individually identifiable information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to a consumer . . .”. The definition of personal information should be clarified to provide more specificity.

### Access and Correction

Version 1.2 still includes inconsistent response times for access and correction. As previously noted, many of the included response times are significantly shorter than Model #670, HIPAA, and what is required by state laws such as the CCPA/CPRA. Operationally, it would be very challenging for insurers to comply with these reduced time frames, which would provide little benefit for consumers. Additionally, Version 1.2 continues to contemplate that insurers will annually provide a list of all third-party service providers who receive personal information. As ACLI previously suggested, this should be revised to require, upon request, disclosure of the categories of persons who receive personal information, consistent with state laws such as the CCPA/CPRA.

There also remains a lack of clarity in how the timing and verification obligations are to be achieved with the expansion of these rights to third party service providers and publicly available information. The obligation should be on the consumer to correct publicly available information at the source and inform the licensee once the correction has been made.

### Notice- Timing, Content, and Delivery

The Working Group has missed this opportunity to modernize and embrace steps taken by other regulators to meet the modern delivery demands and the sustainability expectations of consumers, where paperless digital delivery should be the default method unless the consumer requests the notice be mailed in hard copy format. Version 1.2 requires multiple disclosures and notices that will be lengthy in nature and require additional delivery requirements and confirmations, ultimately causing an increased burden to the customer given the confirmation receipt processes. Some of these changes would increase complexity, cost, and the number of notices individuals receive, all at a time when the trend is to decrease the frequency of notices or provide them by alternative means. Customers want clear, simple, digital experiences. The overly prescriptive requirements are complex and will cause confusion to the consumer. In addition, it continues to be a security concern that a consumer can request a list of all third-party service providers the insurer shares personal information with. As raised during the in-person meeting in Kansas City, this will provide a roadmap to malicious actors.

### Nondiscrimination and Nonretaliation

Section 15 A (1) and (2) includes a rebuttable presumption that a licensee has discriminated or retaliated against a consumer if the consumer is required to consent to an “additional activity” to obtain a particular product, coverage, rate or service or transaction. The inclusion of the undefined term “additional activity” creates a vague and unclear standard on which to base a rebuttable presumption. Further discussion is needed on what “additional activity” refers to in order to fully evaluate whether a rebuttable presumption is appropriate.

### Consent Versus Authorizations

As currently written, the draft conflates opt-ins and opt-outs with authorizations. Existing law allows customers to opt-in to certain types of information sharing. This is a onetime opt-in unless revoked. An opt-in is a straightforward process that could involve a check box or a simple affirmation. An authorization, on the other hand, requires certain language, such as an expiration date, the type of data, the identity of recipients, and the specific purpose of the authorization. This concept might make sense and be well understood in the context of Model 672's language regarding disclosure of nonpublic personal health information. By conflating opt-ins with authorizations for all lines of business, this draft unnecessarily complicates the opt-in process. It would likely cause licensees to forgo opt-ins altogether because it would require the creation of a burdensome administrative process for expirations, among other reasons.

In addition, the draft also requires an authorization for an opt-out process for information sharing or participation. An opt-out provides a consumer the opportunity to remove the information sharing or participation in the event or activity that is occurring. It is not a consent process and should not require an authorization. If authorization were required, it would therefore be an opt-in or consent process. The requirement for authorization or consent for opt-out processes should be removed.

### Reinsurance Concerns

Version 1.2 appears to include non-licensed, non-affiliated reinsurers in the definition of third-party service providers. If that interpretation is correct, the requirements for third-party service providers would apply to situations where licensed cedants ceded to non-affiliated, non-licensed reinsurers, and thus it would still apply to reinsurance. Additionally, while the draft appears to exempt reinsurers from the consumer notification requirements, this exemption is incomplete. Section 8A(1) needs to be replicated under 8B, 8C, 8D, 8E. Or, a simpler solution may be to delete 8A(1) and create 8F, and transfer the reinsurer exemption there.

### Group Insurer Concerns

Draft Model #674 continues to impact long-standing practices around administration of group insurance business. Current law allows licensees to provide initial, annual, and revised notices to the plan sponsor, group or blanket insurance policyholder. Without these provisions, insurers will be in violation of the law when, for example, an employer automatically purchases insurance for an employee and provides that employee's personal data to the insurer.

### Conclusion

Consumers and companies need consistent privacy rules providing equal protection across the country. A patchwork quilt of differing state-by-state or sector-specific privacy regulations is confusing, frustrating, and not helpful to consumers. While modernization of existing privacy laws should be undertaken as advances in technology support collection and analysis of an ever-increasing amount of personal data, regulatory proposals that would unnecessarily increase complexity must be avoided. Additionally, while some aspects of insurance and financial services is unique and reflects the need for a unique regulation, it is important to have some harmonization with other privacy regulatory schemes so insurance does not end up with conflicting and contradictory aspects of handling personal information.

It is critical that we give the Model #674 drafting process the time it warrants to ensure the final version is carefully crafted to strike a balance between protecting consumer privacy and enabling insurers to meet the needs of their customers effectively.

Thank you for your consideration of our comments. We welcome any questions.

Sincerely,

A handwritten signature in cursive script that reads "Kristin Abbott". The signature is written in black ink on a light-colored background.

Kristin Abbott  
*Counsel*

A handwritten signature in cursive script that reads "Jennifer M. McAdam". The signature is written in black ink on a light-colored background.

Jennifer M. McAdam  
*Associate General Counsel*



**John Euwema**  
VP-Legislative/Regulatory Counsel  
1300 Pennsylvania Ave, NW 190-327  
Washington, DC 20004  
630.824.7300

July 28, 2023

Katie Johnson, Chair  
Privacy Protections (H) Working Group  
National Association of Insurance Commissioner  
110 Walnut Street, Suite 1500  
Kansas City, MO 64106-2197

*Attn: Lois Alexander, NAIC Market Regulation Manager*  
By email: [lalexander@naic.org](mailto:lalexander@naic.org)

RE: CCIA Comments on Exposure Draft of July 11, 2023, of Insurance Consumer Privacy Protection Model Act #674

Dear Chair Johnson,

The Consumer Credit Industry Association appreciates the opportunity to comment to the Working Group on the exposure draft of July 11, 2023, of Insurance Privacy Protection Model Act #674.

We continue to express our concern that the Model Act is expanding its scope of requirements to licensees' non-insurance products and services. The Model Act should apply its requirements only to products that the state insurance codes and state regulators recognize and regulate as insurance products, consistent with other NAIC Model Acts.

Many licensees offer non-insurance products to enable holistic planning for consumer financial security. The state insurance codes exempt, and regulators explicitly recognize as non-insurance, such licensee products as GAP waiver, debt cancellation agreements, service contracts, and motor club products.

Accordingly, to explicitly and clearly exempt from the Model Act a licensee's non-insurance business CCIA recommends that a new subsection D. be added to Model Act Section 1., "Purpose and Scope", as follows:

*D. This Act shall not be applicable to or govern a licensee's collection, processing, retention, use, or sharing of any individuals' information involving or in connection with non-insurance products or services.*

We make this recommendation considering that the current exposure draft seems to confirm an intent to regulate non-insurance products offered by licensees in a similar manner as insurance products. The Model Act includes numerous references to financial products and services which by definition are not limited to insurance products.

An example is found in Section 2.V.(6) which may expand the definition of insurance transaction to include offering, selling, or servicing a financial product or service without more appropriate limits to include only insurance products or services regulated as such under the state insurance codes:

*Offering, selling, or servicing of a financial product or service (emphasis added) of the licensee or its affiliates.*

The new Section 2.O defines “financial product or service” without limitation to only products and services regulated as insurance under the state insurance codes further compounds our concern that a licensees’ non-insurance business will be swept into this Model Act.

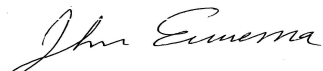
Accordingly, we further recommend that Section 2.V.(6) be removed from the Model Act.

We remain uncertain as to the purpose of all other references to financial products or services and will not address them here. Regardless, the exposure draft in every way or intent needs to limit its scope of regulation to insurance products and not willfully or inadvertently apply itself to products which are not insurance, including those which the licensee may market to or with financial institutions.

The Model Act should, consistent with state insurance codes, clearly exempt non-insurance products from its scope starting with our recommendations to add a new subsection D. to Section 1., and delete Section 2.V.(6).

Thank you for accepting our comments, and we look forward to working with you to provide an effective Model Act that recognizes the complexity and variation of licensees’ insurance and non-insurance products and services.

Sincerely,







July 28, 2023

Chair Katie Johnson  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106  
Via email to [LAlexander@naic.org](mailto:LAlexander@naic.org)

RE: Comments regarding July 2023 Draft of Consumer Privacy Protection Model Law (#674)

Dear Chair Johnson,

The American Property and Casualty Insurance Association (APCIA) appreciates the opportunity to provide initial comments in response to the updated draft of Consumer Privacy Protection Model Law #674.

APCIA is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

We appreciate the opportunity to share APCIA's initial thoughts on this updated draft. Our members are very invested and engaged in this process, as demonstrated by our participation in open calls, national meetings, and the interim meeting, as well as our submission of written feedback at various points throughout the process. We recognize there are incremental improvements in this draft, for example eliminating prior consent requirements for cross-border data sharing. Nevertheless, significant concerns remain with the workability of many of the current draft's requirements.

We have also included a redline with specific language recommendations and will share additional feedback as this process evolves and our members more thoroughly review the text and its potential impacts. We also note that our previous feedback remains unaddressed, and welcome understanding the Working Group's reasoning so that we may clarify our concerns or offer modified recommendations.

During the Working Group's July 25<sup>th</sup> conference call, it was noted that regulators knew this current exposure draft would change and that, in fact, a redline version 1.3 is expected to be exposed in a couple of weeks. Understandably, this is concerning to our members that have devoted considerable time to analyze and suggest drafting language for Version 1.2. An effective collaborative process requires regulators and interested parties to all collaborate from the same document with meaningful time for review.

These issues are complex and we must recognize the necessary interplay with existing state and federal legal obligations as well as cross-sectional alignment within the model itself. As such, it is critical that the remainder of this process not be rushed. Rushing could result in unintended consequences and a Model that cannot be adopted uniformly, if at all. Ultimately, this will only compound the emerging patchwork of inconsistent state privacy laws rather than ameliorate it.

The following significant concerns are intended to be helpful and show that the draft Model has a long way to go before being finalized.

### **Definitions**

Our members noted several changes to definitions in this new draft. We have provided initial feedback on some of those changes here, but our members have not had sufficient time to review those changes in detail. We would request that the Working Group consider focusing one of the upcoming open calls on further discussion of this topic, as the definitions and how they are applied will be critical to how we understand and respond to other provisions of the draft. We have included more thorough revisions in our redline, but a few of the definitions that we recommend changes to or require clarification for include:

#### *“Additional Activities”*

- Although the category of “Additional Permitted Transactions” has been removed, there are repeated and significant references to “additional activities” throughout the updated draft. We recommend that this term be defined clearly, and clearly distinguished from the what activities are considered an “insurance transaction”, also making sure to address any gaps.

#### *“Biometric Information”*

- This should be aligned with the Virginia or California definition, which we have previously provided.
- Additionally, “sleep, health or exercise data” should not be included in this definition.
- We request it be made clear that neither photographs nor videos are biometric information.

#### *“Consumer”*

- Under this definition, a consumer is someone who has engaged in an insurance transaction. That seems to start at quote or application. That will imply that if someone accesses the website, there are no limits to data collection and use, but once the quote process starts, then they are considered a consumer and all rules apply.
- Also- would a worker’s compensation claimant be considered a consumer? We recommend reverting to language in NAIC Model Reg 672-1, which stated that a worker’s compensation claimant was not a consumer if the insurer provided privacy notices to the worker’s compensation policyholder and the insurer did not disclose nonpublic personal information other than as permitted under the regulation. We would also seek clarification on whether a group insurance member would be considered a consumer.

#### *“De identified”*

- California and Virginia already define de-identified information. For consistency’s sake and to ease compliance, we urge the Working Group to pick one of those definitions rather than creating yet another one.

#### *“Insurance Transaction”*

- We have several outstanding concerns with this definition, which are provided in redline. A few primary points are included below.
- We recommend clarifying that a quote is considered an insurance transaction.
- We recommend the deletion of the language “any mathematical-based decision that involves a consumer’s personal information.” As we have raised previously, this language is unclear and confusing and should either be clarified or deleted.

*“Nonaffiliated Third Party”*

- It should be clarified that a third-party service provider is not an unaffiliated third party.

*“Personal Information”*

- We suggest considering deleting all sub-provisions. This would then better mirror the definition of personal data in all other laws.
- It should be clarified that publicly-available information is not personal information, in alignment with the approach taken generally by other comprehensive privacy laws.

**Third Party Oversight**

Although some improvements have been made in this section, the provisions regarding requirements for oversight of third-party service providers remain overly broad and prescriptive. The updated draft includes a number of requirements that it is unrealistic to expect vendors will agree to. One example is the requirement that a third-party service provider is required to comply with each individual licensee’s privacy practices. This is not workable in practice, since a vendor cannot reasonably comply with thousands of companies’ privacy practices. Contractually requiring data usage to be limited to the contractual purpose and compliance with applicable laws should be sufficient. Licensees are also not able to prevent vendors from having subcontractors. The typical limitations for these types of issues are that the vendor can only use the information as provided for in the contract and cannot sell it, which would be a workable alternative.

Our members also note concerns with the implications of including publicly-available information in these requirements, and in other places throughout the draft. It is unclear in this section specifically why a provision related to publicly available information is necessary and, even if so, why is it limited to claims. We recommend not applying the requirements of Section 3(C) to publicly available information. APCIA also recommends aligning Section (3)(F) with the provisions regarding re-use and re-disclosure included in Model 672, which our members believe addresses those topics thoughtfully and effectively. We also recommend several other edits included in-text in our accompanying redline.

**Data Minimization**

APCIA is glad to see that the earlier provision requiring consent for overseas data sharing has been removed. This constitutes a significant and critical improvement to the data minimization section and the draft as a whole. Regarding Section 4(B), such data usage is a common topic in state breach disclosure laws. Several such laws include a thoughtful good faith exemption, explicitly defining it as “not-a-breach” if the insider who sees something they should not makes no inappropriate use of the data. We recommend including such language.

**Sharing Limitations**

APCIA members found this section to be one of the most problematic in terms of remaining issues. First, the provisions included in Section 5 are broader in scope than sharing, as they specifically also address “processing, collection, and retention” as well. We request this section be limited to sharing specifically for additional clarity. Our members are particularly concerned by the requirements outlined in Section 5(A)(8). We note that no other law includes the requirements stated in Section 5(A)(8)(a) and (b). As a general practice, companies are permitted to transfer data without qualification. In particular regarding Section 5(A)(8)(b), during due diligence, a recipient may need to share the information with the recipient’s counsel or other experts. Under this provision, it is not clear if that is even feasible. For these many reasons, APCIA requests these provisions be stricken.

Our members have also raised concerns that the implications of this language for joint marketing do not match the stated intent towards the joint marketing issue that was included in the cover letter. Specifically, Section 5(A)(14) will require edits to more clearly enable joint marketing between financial institutions as authorized by the Gramm-Leach-Bliley Act (GLBA) and subject to the Working Group's intended opt-out requirement. Regarding Section 5(A)(15), marketing of an insurer's own products should be considered an insurance transaction. Also, it is unclear how insurers are expected to provide consumers with an opportunity to opt-out if they haven't interacted yet. Finally, requiring written consent is inconsistent with the notion of an "opt-out" and in effect changes this to an "opt-in" standard. For these reasons, and others, we request Section 5(A)(15) be removed.

Section 5(B) imposes an unreasonable requirement regarding sharing with nonaffiliated third-parties. This requirement may not be feasible, as insurers need to share this information with third party service providers to administer claims and for other insurance purposes. Our members recommend perhaps applying this requirement only to "additional activities", or explicitly allowing such sharing for the purposes of "insurance transactions".

Finally, Section 5(A)(9) suggests that information may be shared with an affiliate only for auditing purposes. Current law allows personal information to be shared amongst affiliated entities, which is necessary to the operation of insurance holding company systems. There are other legitimate reasons to allow sharing with affiliates to conduct usual and customer insurance and related transactions.

### **Consumers' Consent**

Regarding consumers' consent, our members had several recommended changes to these provisions. First, it is critical that this section has a clear exception for detecting or preventing fraud. The language in Section 5(A)(6) would work well and could be replicated here. The language of this section also does not currently make clear that consent may be provided electronically. We recommend including clarifying language that allows consumers to provide consent electronically or verbally, in addition to in writing.

In addition, APCA strongly recommends that Section 6(B) be updated to align with the relevant provision from either the Virginia or California privacy law. Our members also have concerns with the amount of detail required for consent. That level of detail will require a long form that will not be digestible and will undermine efforts towards clarity. For example, listing all the underwriting companies isn't entirely helpful when they think of the company as its commonly-known, primary-brand name. Most existing privacy laws focus more on explaining the purpose and use of the data, rather than these additional factors for consent. We recommend that approach. If this section is largely retained, we recommend at minimum combining Sections 6(B) and 6(C) into one consolidated set of requirements and process for consent for additional clarity.

### **Retention and Deletion**

APCA has significant concerns with this area, which is in our members' view currently one of the most unworkable parts of this draft. Our primary issue concerns Section 7(B), which requires a licensee to review all of a consumer's personal information in its possession, in addition to its retention schedule, and to determine whether the reasons for collecting or processing that information remain. This is a completely unworkable requirement. It is not feasible for a company to review all consumer personal information in its possession on an annual basis. This provision also suggests some misunderstanding about how insurers' retention schedules work. They are not based on a person, but rather, are based upon categories of business records. For example, claims business records are retained for a certain number of years from the date the claim is closed. A consumer's claim information may be retained for a longer or shorter period of time than their policy information. For those reasons, all of a consumer's data will not be ready to be

deleted on the same day or even necessarily in the same year. A company can review the retention schedule annually to determine if it is compliant with existing laws, which is a much more reasonable alternative.

In terms of other issues, Section 7(A)(2) should be broadened to compliance with any legal obligation, not only those involving certain types of transactions. Insurers are required to meet all of their legal obligations and the language of this draft should not prevent them from doing so. Section 7(C) also seems to rely on the idea that insurers are making constant individualized determinations, which is not how these processes work in practice. It is a positive change that this draft recognizes that some systems will not allow for deletion or deidentification. However, several subsections of this provision still seem to have a disconnect from some of the operational realities of insurers' business models and the limitations of legacy systems. We have further elaborated on these areas in our redline and recommend language changes to address those concerns. In Section 7(C)(3), there is also an unrealistic time frame required for transitions from legacy systems. APCA suggests including language to make this more adaptable as is appropriate. Finally, Section 7(C)(4) imposes an impractical and unrealistic requirement for third-party providers. First, many contracts with third-party providers explicitly require those providers to preserve data beyond the contract termination date in order to comply with legal retention obligations. As worded, this clause in the Model Act would have the effect of voiding those survivorship clauses. Second, third-party providers have the same practical limitations to deletion as insurers do. Data is interlinked, backed up and handled in complex ways that cannot be simply undone on the very same day as a contract ends. This is especially true if contract termination is unscheduled.

Finally, third-party service providers may have independent relationships with the consumer (e.g., car rental companies, banks, body shops, etc.) and may not be able to follow insurance industry practices or these rules without undue hardship. This will greatly reduce the service providers available for use by insurers.

As such, we recommend this provision be truncated to note that third party service providers shall delete such information as soon as is reasonably practicable. For that same reason, we also recommend that Section 7 exclude data stored in backups.

### **Notices and Delivery of Notices**

There are several areas APCA would like to highlight regarding the requirements for both content and delivery of notices.

Section 8(B)(1) impacts joint marketing. This provision could require an insurer to send privacy notices as soon as the licensee receives a consumer's information from a joint marketing partner financial institution. That sharing is covered by the other financial institution's privacy policy and notice already sent to the consumer. The notice may be required even if the insurer never markets or shares the consumer's information, which would likely cause consumer confusion. We request the language be updated to better reflect the intent expressed in the cover letter to permit joint marketing agreements. Our members also noted an additional practical concern with this requirement. The provision states that the initial notice must be given when the insurer first collects the personal information. In order to give the initial notice, a licensee can rely on having a privacy notice on the website, but the consumer has to agree to accept notices electronically under the UETA before the electronic privacy notice is delivered. This constitutes a practical problem. Once again, we recommend reworking this provision if it is retained.

In addition, the requirements of Section 8(C) and (E) should include a materiality trigger. This seems more consistent with the intent expressed in the cover letter and throughout the rest of the draft. Regarding

Section 8(C)(2), it is not feasible for licensees to provide a privacy notice to third-party claimants and beneficiaries, for a number of reasons. Insurers may not have sufficient contact information for these individuals, and in many cases, beneficiaries are not aware that they are a beneficiary. This means a licensee may have to explain its relationship to them, as the individual will not know. This is unnecessary and would cause confusion. We recommend removing this provision.

We would like to raise again a concern with the language of Section 9 that was mentioned in the interim meeting, as well as in earlier comments. The language around notices in Section 9 refers to a “list of persons” as opposed to “categories of” sources or third-party service providers. APCA reiterates our position recommending that this language refer to categories rather than a list of individual persons. It is not only likely infeasible, but also a security risk to share a list of specific persons and third parties with whom a consumer’s information was shared. This could also create confidentiality concerns.

We recommend the provision Section 9(A)(7)(b) be limited to apply only to sensitive personal information. Regarding 9(A)(10), it will not be feasible to adequately explain the complexities of complex insurance retention policies in this context, especially given the extensive and worsening patchwork of legislative and regulatory requirements insurers are subject to. This requirement also has the unintended consequence of undermining the requirement that notices be clear. We suggest a more reasonable alternative in our redline language. Regarding Section 10 on the whole, it seems unnecessary to create a separate privacy notice that must be sent to consumers annually when the notice addressed in Sections 8 and 9 is not required annually unless there are material changes. For this reason, we recommend consolidating all of this information into one notice, to be provided on the same schedule as the notice referenced in Sections 8 and 9.

Section 11, regarding delivery of notices, also has a number of outstanding issues. In present form, it does not address what happens when a consumer is interacting via telephone. In addition, this section only makes sense if the only “consumers” are insureds, but would make little or no sense in the context of claimants, witnesses, commercial-insured employees, etc. As mentioned in our feedback on the definitions, further clarification on who is a “consumer” under this Act is necessary for this to work. Our members also recommend combining Sections 11(C) and (D) into one clear, consolidated provision. 11(D) is more clearly written, so we recommend merging 11(C) into 11(D), making the language of 11(C) exceptions in the new combined provision.

APCIA would like to reiterate our members’ concern regarding the requirements for delivery receipts, which we raised in our comments on the initial draft, on an open call and in the interim meeting in Kansas City. No other privacy law or industry requires proof of receipt for notices and the expectation that consumers would provide such a receipt electronically or otherwise. Moreover, as we raised in our previous comment letter, many email systems do not return read receipts, and users can turn off the sending of read or sent receipts. It is also unclear how a consumer would acknowledge receipt of viewing the notice on the website. In addition, no equivalent ‘proof of receipt’ is required for paper delivery and we do not see a clear reason to require a higher standard for electronic delivery. The requirement for delivery receipts is both unnecessary and infeasible, and we continue to recommend it be removed.

#### **Access to Personal and Publicly Available Information**

Section 12(A) should be narrowed to a more appropriate scope. It is feasible to make a request for data that the third party has under a contract with licensee, not just all of the data that the third party has about a given consumer. Our members also oppose the inclusion of publicly available information in this section. Including publicly available information here would require disclosing every piece of information an insurer possesses about a consumer, whether or not the insurer relies upon that information. This is unnecessary.

Insurers are already required to explain adverse underwriting decisions and claim denials. For these reasons, we suggest moving this provision to Section 14 (if that Section is retained) and allowing consumers to see “publicly available information” if it was used in reaching an adverse underwriting decision. Additionally, it is unclear what Section 12(E) is intended to address. These requirements should be limited to consumers.

Although the time frames in Section 12(B) are improved, they are still not uniform with California. We would recommend fully aligning them with what is required in CPRA, which references “calendar days” rather than business days, and includes language to allow for an additional 90 days if needed.

#### **Correction of Personal and Publicly Available Information**

Our members have various concerns with the obligations imposed and approach taken regarding correction. The obligation that licensees and their third-party service providers correct publicly available information is problematic. Despite the efforts in Section 13 to detail a refusal process, this obligation puts licensees in the inappropriate position of disputing information prescribed in government records with consumers.

We recommend an alternate approach to addressing publicly available information- to reference a licensee’s obligation to correct internal records once the relevant government office has amended the consumers’ information. It should be the consumers’ obligation to provide licensees supporting documentation from the government office to evidence this change. Additionally, some data must be verified before insurers can make a change, and some changes will affect the premium and require complete recalculations, possibly even re-underwriting of the policy. Those processes take time and 15 days is completely unworkable from that perspective.

The timeframe in this section should mirror the timeframe for access in Section 12. We emphasize that these time periods are even more unrealistic if the requirement to correct publicly available information is retained. We recommend the changes suggested for the timelines in Section 12 above also be applied here.

Section 13(B)(2)(b), requiring a specific legal basis to not correct information, is also problematic. Our members would like to know if accuracy would be considered a legal basis in this context. We note that the CPRA regulations provided details around correction that could be utilized as a template to clarify this Section and help harmonize requirements. In general, we believe more flexibility is necessary. The remedies suggested in 13(D) and (E) are more appropriate to strike the right balance.

As a best practice, consumers should start the correction where the actual bad data originated. Then, following the procedure outlined, they should pass it downstream to the licensee. This is a more effective, efficient and appropriate system.

#### **Adverse Underwriting Decisions**

Although Model 670 includes provisions related to Adverse Underwriting Decisions, APCA recommends this content not be included in this updated Model. Currently, there are other state laws that govern this area effectively. This was likely not have been the case when Model 670 was drafted, which would explain the topic’s inclusion here at that time. Since the legislative landscape has developed to more appropriately address this in other places, this content no longer belongs in the privacy Model. We recommend removing this section from the Draft. Should this Section be retained, however, APCA has included several in-line language suggestions in redline to improve its workability.

**Sections 16-20**

APCIA previously submitted comments on these Sections for consideration. We would request that those comments still be considered with respect to the new Draft.

**Sections 33**

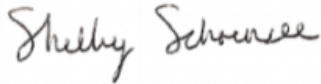
We believe that a transition and delayed enforcement period will be necessary. Our members request three years minimum to implement these provisions, and potentially will need longer for the provisions regarding third-party service providers.

**Conclusion**

APCIA thanks the Working Group for its hard work and continued engagement on this project. We remain committed to providing constructive feedback and respectfully urge the Working Group to not rush this process.

We welcome the opportunity to discuss these concerns and recommendations with the Working Group.

Sincerely,

A handwritten signature in cursive script that reads "Shelby Schoensee". The signature is written in black ink on a white background.

Shelby Schoensee  
Director, Cyber & Counsel





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

**NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS  
PRIVACY PROTECTIONS (H) WORKING GROUP**

***New Consumer Privacy Protections Model Law #674  
Version 1.2 (July 11, 2023 via calendar posting; July 28 Comment Deadline)***

Given the problematic content of version 1.2 (a fully new version), the ambitious workplan schedule, and the potential impact of the massive magnitude of the task before them, the **National Association of Mutual Insurance Companies (NAMIC)<sup>1</sup> members respectfully urge the Privacy Protection Working Group (PPWG) and the National Association of Insurance Commissioners (NAIC) to pause and reassess gaps and this project; and, if moving forward, to reset with a targeted and well-defined scope that leverages a common framework.** By prioritizing a tailored model proposal that addresses a defined gap, the NAIC may be less likely to risk unintended and disruptive consequences resulting from a significantly broader draft.

While these comments are unavoidably critical of pending version 1.2 and skeptical of the ability of the NAIC to finalize a workable model (especially on the schedule reflected on the workplan), **NAMIC very much appreciates the PPWG engagement with interested parties since the initial exposure draft was released in February. From the two day in-person meeting in Kansas City in June to several conversations, there is no doubt of the group's dedication to the model effort or time commitment.** Unfortunately, at this time the NAIC appears to be at the precipice of advancing down a path toward near-final stages of a model drafting effort that would require substantial edits to approach and careful edits to wording in order to near being workable. After many months, few of the comments NAMIC shared about structure and operations and little of the specific language to largely accomplish the PPWG's aims (with less disruption and expense) were reflected in version 1.2. Therefore, with only a couple of months between the Summer National Meeting and the deadline to finalize the model's content, NAMIC must deliver these difficult messages.

---

<sup>1</sup> NAMIC Membership includes more than 1,500 member companies. The association supports regional and local mutual insurance companies on main streets across America and many of the country's largest national insurers. NAMIC member companies write \$323 billion in annual premiums. Our members account for 67 percent of homeowners, 55 percent of automobile, and 32 percent of business insurance markets. Through our advocacy programs we promote public policy solutions that benefit NAMIC member companies and the policyholders they serve and foster greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.



## Reassess needs and define the scope.

**Identifying a targeted and compelling gap should be an essential precursor to NAIC model drafting activities.** With due respect, the question should be asked, using Model #672 as a consistent starting point – and considering both some of the comprehensive privacy laws that have been passing in the states and the specific context of the insurance product/relationship — what should be the scope and focus of regulator-driven legislative efforts? In conducting such a review, policymakers might determine that an appropriate way to define a targeted scope of model language might be stand-alone wording to address a particular identified a gap which necessitates legislative action.

Unfortunately, the pending version 1.2 would throw out the structure insurers have been working under. Instead, the PPWG could modernize from the universal baseline of #672 (as discussed below), after a determination of need/gap. While still discussing the idea within membership, this might potentially address consumer requests similar to the new comprehensive states (rather than exporting the old #670 approach or to the new draft wording in version 1.2). Again, the foundational baseline for additional requirements should be what is in place today.

## Reframe the substantive starting point.

**Working from the baseline substance contained in Model #672 is the most sensible foundation on which to build additions to the privacy framework to which insurers are subject.** First, the content of this successful NAIC model is in place countrywide, so there is relative consistency in those provisions. And therefore, using it as a foundation would seem to better avoid some disruption and implementation challenges. Second, using #672 also benefits from a fairly level playing field, with relative consistency across financial institutions, which is essential considering the reality of being part of the broader sector, consumer expectations, and federal law. It would also avoid risks to joint marketing (where the wording is an area of ongoing concern) as well as to other areas such as the mechanics of notice/options at new business (which is among a long list of concerns). Third, it is understood for purposes of compliance and enforcement. A large rewrite (even of uncontroversial provisions) threatens introducing potential confusion and questions (by legislators, regulators, licensees, or courts) about the relevance of wording differences. In sum, consider working from and making targeted changes to requirements in place across the country rather than creating a wholesale replacement (with problematic wording: internal inconsistencies, unworkability, frustration of consumer purposes, and vast interpretation and clarity challenges).

**NAIC Models are intended to serve the purpose of enhancing uniformity,<sup>2</sup> yet as drafted rollout of this model may have the opposite effect.** A state that passes this as is may be a significant outlier, creating inconsistency. (And depending on interpretation, it may possibly invite federal involvement as it explicitly indicates that it would “supplant” notices required under Gramm-Leach Bliley.) Indeed, version 1.2 differs not only from existing NAIC models and GLBA, but also from anything else that exists today.

<sup>2</sup> <https://content.naic.org/cipr-topics/naic-model-laws#:~:text=Issue%3A%20The%20NAIC%20model%20law,judicial%2C%20legislative%20and%20regulatory%20frameworks.>



**Reconsider the schedule; the workplan does not provide adequate time to get it right.**

**Being locked into the timeline displayed on the Workplan underestimates the amount of work necessary and undervalues the importance of the work product.** NAMIC urges the NAIC to reconsider its current trajectory for a vast overhaul of insurance-related state privacy laws/regulations.

**As it now stands, substantive problems abound in the Version 1.2 redraft.** The pending version 1.2 draft is not at the stage of requiring simple or minimal edits. While some regulators on the PPWG may have seen many versions of its drafting efforts, version 1.2 is only the second full version that has been released for exposure and it is a complete rewrite from the earlier draft (with some concerns carried forward from the prior draft and some newly created). While there were some incremental positive changes from the initial exposure draft (for example in the area of international sharing), many problems remain. It appears to be a far distance from being workable and cohesive.

**Precedent supports for additional iterative drafting/time** on important projects. At the NAIC, even on the more straightforward effort for cybersecurity with the Insurance Data Security Model Law (#668), the drafting process allowed for numerous exposures for public comment, finalizing and ultimately adopting after six or more drafts.<sup>3</sup> While ultimately not all the issues were resolved in that model process, the more iterative drafting process likely helped to craft a work product that potentially reduced the volume of issues debated/revised before legislatures. Indeed, the history of the Pet Insurance Model Act (#633) reflects the willingness of leadership to extend time and to allow for additional work to endeavor to resolve concerns.<sup>4</sup> International precedent also supports taking more time to draft in this area. For example, the foreign General Data Protection Regulation (GDPR) was in development over a long period of time, with what appears to be three to four years between the release of its first draft proposal and its adoption.

**Not asking for delay for delays sake**, good faith engagement characterizes NAMIC's involvement. Not only did NAMIC staff and members attend two days in Kansas City along with the PPWG trying to explain challenges and work through issues, we also have been actively involved outside that venue, sharing concerns, wording, and rationale. NAMIC appreciates the PPWG's willingness to engage in discussions regarding the February initial exposure draft and acknowledges that the PPWG has been working diligently and earnestly. Although NAMIC has been eagerly awaiting a redraft, seeing the new version 1.2 offers little confidence that a worthwhile national sector-specific privacy model can be developed in the few months after the Summer National Meeting.

<sup>3</sup> <https://content.naic.org/sites/default/files/model-laws-project-history-668.pdf>

<sup>4</sup> <https://content.naic.org/sites/default/files/model-law-project-history-633.pdf>



## Recognize that the substance of pending version 1.2 draft is highly problematic.

While there seems to be intent to improve from the initial exposure draft version, and in some ways, it appears to move in a positive direction, **the draft does not fully address situations and in some cases version 1.2 introduces new confusion** (and technically the draft language does not fully comport with the cover page). There have been some changes in areas like marketing, affiliate sharing, cross-border sharing, additional permitted transactions, and research activities. Yet, NAMIC members indicate that in some of these areas the improvement is incremental and may either only partially resolve issues or may introduce others. While version 1.2 treats marketing more reasonably as an opt-out rather than an opt-in (in most instances), the model would still limit direct marketing. Specifically, it appears to limit the ability to engage ones customers in a discussion of risk, risk management, risk mitigation, and related insurance products/options. This harms customers. See. Sec. 5(a)(15). And it also is not directly considering other protections that currently exist under the law (not aligning with FACTA affiliate marketing). While version 1.2 removes the initial exposure draft prohibition on affiliate sharing, it remains unclear about it in the context of an “additional activity.” This is an area of great concern. Although “additional permitted transactions” itself has been removed, the draft still radically endeavors to create two buckets (insurance and other undefined additional activities) and to restrict based on where a task falls. This creates an entirely new approach which is unnecessarily confusing, unknown, and far from the construct that is known to insurers (and financial institutions more broadly) as well as to regulators. With respect to research activities, while NAMIC does not support the overall construct, if it is the direction of the group, the version 1.2 approach and definition seems to address many of the preliminary concerns and NAMIC does appreciate that change, which aids in understanding. In totality NAMIC members do not feel with confidence that the draft is ultimately better than the earlier one because of the confusion about many provisions and wording. This is fueling concerns about timing and the novel approach.

**Review previously submitted comments and suggestions**, please. The vast majority of practical and reasonable concerns expressed by NAMIC were not addressed and are carried forward into version 1.2. Importantly, to the extent the PPWG is not using #672 as its foundation, NAMIC urges the PPWG look to reasonable and existing guides to aid operational stability. Largely, these were the sources that underpinned the very detailed suggestions provided previously. When it comes to things like notice<sup>5</sup> (content, timing, and delivery), logistics/processes around consumer requests,<sup>6</sup> exceptions (including fraud, which has not been thoroughly addressed, as well as other necessary items), preferences approach and mechanics (opt-out/in), record retention requirements (which are based on complex laws around different types of business records), and many definitions (which are critical to the entire document), it is imperative to align with certain existing requirements, recognize the investments already made to build structures and processes to comply with requirements (for those doing business in certain jurisdictions); value the lessons learned from those experiences; and understand that some companies have not already built for complying with certain states where they do not do business (California, for example)(so they may need more time and flexibility in the transition). Further, some of the previously shared comments/language focused on feasibility of expected requirements on third party service providers. For

<sup>5</sup> Again, a unique list of every single TPSPs under Sec. 9(A)(5) cannot be identified in all instances – please refine to focus on “categories.” This is just one example of remaining items.

<sup>6</sup> For example, consider timing; the need for clarity around “verifiable request” (as used in Sec. 12(A) (see suggested definition previously provided)); the need for the response to include “categories of persons with whom we may have shared” (under Sec. 12(B)(2)(a)); taking the approach of providing a summary as under CCPA (see Sec. 12(B)(2)(b)) rather than creating a new expectation; and removing the additional notice informing the customer that the licensee has followed consumer instructions (under Sec. 12(C)).



example, whether in the initial exposure draft or in version 1.2, all vendors should not need to (or they would not) agree to comply with each company's privacy practices (which may address a wide range of situations and data beyond the scope of the contract with the TPSP). Further, licensees should not be expected to act as enforcers of the law by "requiring" TPSPs to do something. However, if the PPWG is looking for insertion of new contractual provisions with TPSPs pointing to compliance of the law, that is a more reasonable way to frame that requirement (though as highly stressed earlier, ample time must be provided for contracts entered or renewed after a particular date). Again, we re-offer the previously offered comments and language as they remain relevant for many of the operational challenges.

**Remove provisions that are not privacy-specific or private information**, which would narrow the scope and reduce open issues. Please consider a few examples. When it comes to legacy systems (Sec. 7(C)(2)(b)), the systems/technology that an insurer uses and how they secure them is more of a cyber or IT issue. (And understand that more broadly, the deletion provisions call for further attention.) For transparency in rating/underwriting or "adverse underwriting decisions" (Sec. 14), as a general matter, this seems to: better connect to work of the Property and Casualty (C) Committee; not be necessary for purposes of connecting to Model #670 because so much has changed in this area since the 1980s; and be the topic of NCOIL efforts. Further, please reconsider sweeping publicly available information within the "personal information" definition (Sec. 2(DD)(h)) and the requirements of this model. (And if moving forward, consistent with the point above, generally the "personal information" definition should be relatively consistent with how legislatures have been framing it through the recent comprehensive privacy laws.) Debate over these kinds of issues is taking attention from other essential concerns; please take some of these kinds of issues off the table by resolving them in in the next version.

**In summary, NAMIC urges the NAIC not to rush forward before: (1) reassessing approach (based on needs/scope and using #672 as a foundation); and (2) legislative wording is refined and ready.**

**Writing legislation/regulation – especially something of this magnitude – takes time and exposure. Words matter and models can be on the books for decades.** While some problems from the initial exposure draft that were tackled in version 1.2 seem to be moving in a positive direction, not all are fully resolved and new questions and lack of clarity has emerged. Even with many stakeholder conversations, the craft of drafting takes many versions and time.

Concerns are not limited to more drafts and time. **Merging two existing NAIC privacy models at the same time as incorporating ideas from a variety of other state, federal, and international sources (as well as some completely new concepts), the Working Group currently is undergoing an enormous task.** The project has become massive. However, by and large, the existing insurance sector-specific privacy laws work well. **To the extent regulators identify a specific new aspect of privacy to address in a modernization effort, that tailored approach – potentially as a supplemental and cohesive module to attach to what is in place today – may be a more manageable project that may not risk disruption and confusion.**



NAIC Models are intended to serve the purpose of enhancing uniformity. Today, Model #672 is a success, with all states countrywide having those requirements in place. To work swiftly, with minimal disruption, and greatest uniformity, the substance contained in #672 would serve as a strong and consistent foundation on which to build. If a particular discrete topic is identified as necessary, an additional new Article could be added to that model. Of course, the content will be important, but **starting from a baseline all states use today (#672) should not only be less disruptive, but it should also be less of a challenge to uniformity than a completely new model (which may create outliers).**

Version 1.2 takes a novel approach to privacy which would discard the structure insurers have been working under – the one that at a high-level aligns with other financial institutions – and would replace it with something that is being called “radically different” (with many practical questions, including those about “additional activities”). And many other substantive and important issues also remain with the draft. When the PPWG was formed and throughout the process since that time, NAMIC has underscored the importance of workability. **Today workability remains a crucial part of our message.** With all these points as the backdrop, NAMIC respectfully urges the NAIC to pause to assess timing, direction, and scope.

NAMIC has been engaged regularly in good faith through this process and we remain committed to continuing to do so. We expect to share additional thoughts on wording with the PPWG as the process moves forward, though it would be extremely helpful to understand the hesitation the PPWG has to making previously suggested changes. Again, in developing model privacy legislation, time for reviewing the approach and a process to carefully craft its provisions is essential to a successful outcome.

**We appreciate your consideration of these comments. Thank you.**



*Electronically Submitted to lalexander@naic.org*

July 28, 2023

TO: The NAIC Privacy Protections (H) Working Group (the “Working Group”)

**Re: Exposure Draft of New *Insurance Consumer Privacy Protection Model Law*  
#674 – Version 1.2**

Dear Members of the Working Group:

On behalf of our members, the Insured Retirement Institute (IRI)<sup>1</sup> writes to share comments on Version 1.2 of the Exposure Draft of the new Insurance Consumer Privacy Protection Model Law #674 (the “Exposure Draft”). We appreciate the Working Group’s continued efforts on this important issue and commend the Working Group for making important and necessary updates since the last version. For example, we support the updates to Section 26 (Individual Remedies) regarding the private cause of action and the removal of the prohibition on cross-border sharing of consumers’ personal information. We would like to take this opportunity, however, to highlight some remaining concerns for our members:

- 1) **Section 11. Delivery of Notices Required by This Act:** While we appreciate the Working Group’s amendments to this Section, we urge the Working Group to consider additional updates that better align with consumers’ expectations of being able to conduct business electronically. Specifically, in Section 11.B.(3), we recommend that this language be updated to remove the requirement for a delivery receipt for a licensee that chooses to email a notice to the consumer. If a licensee emails a notice to an email address that the consumer has provided (the email address of record), then this should be sufficient to provide actual notice. We see this as analogous to mailing a paper copy of notice to a physical address of record; no delivery receipt is required for a hard copy, and we believe the same should be the case for electronic delivery of a notice.

We’d also ask that the Working Group consider making electronic delivery the default option, with consumers “opting out” of electronic delivery if they wish to receive paper.

---

<sup>1</sup> The Insured Retirement Institute (IRI) is the leading association for the entire supply chain of insured retirement strategies, including life insurers, asset managers, and distributors such as broker-dealers, banks and marketing organizations. IRI members account for more than 95 percent of annuity assets in the U.S., include the top 10 distributors of annuities ranked by assets under management, and are represented by financial professionals serving millions of Americans. IRI champions retirement security for all through leadership in advocacy, awareness, research, and the advancement of digital solutions within a collaborative industry community.

July 28, 2023

Page 2 of 2

We understand that there will always be some consumers that want paper, and this approach will not take that away from those consumers. An electronic default approach (1) is more aligned with increasing consumer expectations that more business (beyond just insurance) be conducted electronically, (2) gives regulators and companies tools, such as detailed audit trails (which paper currently lacks), to identify and deter fraud, and (3) is more environmentally conscious. Moreover, we note that this approach would align with the actions of federal regulators and federal programs that now facilitate greater use of electronic delivery, including, for example, when the Department of Labor used its exemption authority under the Electronic Signatures in Global and National Commerce Act (“E-SIGN”), to allow employers to post retirement plan disclosures online or deliver them to workers by email as a default.<sup>2</sup> We urge the Working Group to consider adopting this approach in its next draft.

- 2) Within **Article III. Notices and Delivery of Notices**, we request that the Working Group add a section regarding Privacy Notices to Group Policyholders by including language from Section 10 of NAIC Model #672. Many carriers currently rely on this language to send notices to retirement plan sponsors who then send them to the plan participants. Taking away this language would impose an unwieldy burden on recordkeepers and may cause confusion for participants who are used to receiving communications directly from a plan sponsor.

We are still discussing the draft with our members, but we understand that the Working Group will be accepting comments until August 7<sup>th</sup>. If there are any additional comments, we will share them by that date. We appreciate the Working Group’s consideration of these comments, and please don’t hesitate to contact me with any questions or concerns.

Sincerely,

*Sarah E. Wood*

Sarah Wood  
Director, State Policy & Regulatory Affairs  
Insured Retirement Institute  
[swood@irionline.org](mailto:swood@irionline.org)

---

<sup>2</sup> See, e.g., *Default Electronic Disclosure by Employee Pension Benefit Plans Under ERISA*, 85 FR 31884 (July 2020), p.9, at <https://www.dol.gov/agencies/ebsa/laws-and-regulations/laws/erisa/new-electronic-disclosure-rule>.





**J. Kevin A. McKechnie**  
Senior Vice President and Executive Director  
ABA Office of Insurance Advocacy  
kmckechn@aba.com  
202-663-5173

**July 28, 2023**

Ms. Katie Johnson  
Chair  
NAIC Privacy Protections Working Group  
NAIC Central Office  
1100 Walnut Street, Suite 1500  
Kansas City, MO. 64106

Attn: Ms. Lois Alexander, NAIC Market Regulation Manager  
*Sent via email:* lalexander@naic.org

**RE: Draft Insurance Consumer Privacy Protection Model Law #674 – Comments of the American Bankers Association’s Office of Insurance Advocacy**

Dear Ms. Johnson:

Thank you for the opportunity to comment on Version 1.2 of proposed Model Law #674 (the “Exposure Draft”). The American Bankers Association (“ABA”) appreciates the Privacy Protection Working Group’s (“PPWG” or “Working Group”) efforts in trying to address some of the issues we raised in our April 3, 2023, comment letter, our one-on-one meeting in early May, and our oral comments at the PPWG’s meeting in Kansas City.

However, we remain concerned that the application of the opt-out requirements for joint marketing to depository institutions and their insurance affiliates is preempted under the Gramm-Leach-Bliley Act (“GLBA”) and the Supreme Court’s decision in *Barnett Bank*.<sup>1</sup> While we are still reviewing Version 1.2, we believe similar federal preemption issues exist with respect to several other provisions. We are again bringing these issues to you so the lack of an exemption for depository institutions and their insurance affiliates does not impede your work as a whole.

*Barnett Bank* was a watershed for the banking industry. It recognized the public benefits associated with national bank entry into insurance sales, and it stopped other discriminatory State insurance laws aimed at national banks. Congress subsequently codified the *Barnett Bank* decision in GLBA and applied the *Barnett Bank* standard to all depository institutions *and their affiliates*. If implemented in its current form, Model Law #674 would disrupt the delicate balance Congress put in place over 30 years ago between the preservation of state insurance regulatory powers and the establishment of limits on those powers with respect to depository institutions.

For these reasons, we urge the Working Group to exempt depository institutions and their affiliates from the Exposure Draft.

---

<sup>1</sup> *Barnett Bank, N.A. v. Nelson*, 517 U.S. 25 (1996).

## I. For Depository Institutions and their Insurance Affiliates, the Barnett Bank Case and GLBA Govern When a State Law is Preempted

While the GLBA permits states to provide greater privacy protections under state law in certain circumstances,<sup>2</sup> it created *separate preemption standards* for state laws that apply to depository institutions engaged in the sale, solicitation or cross-marketing of insurance.<sup>3</sup>

In the 1996 *Barnett Bank* case, the United States Supreme Court held that a federal banking law that permits national banks to sell insurance from small towns preempted a Florida insurance law that prohibited affiliations between financial institutions and insurance agencies. To determine whether preemption was appropriate, the Court examined the authority for national banks to sell insurance. The Court said that the authority was “a broad, not a limited, permission.” The Court then said that the Florida statute is preempted, because it stood as “an obstacle to the accomplishment and execution of the full purposes and objectives of Congress” in permitting national banks to sell insurance. Further, the Court said that a state may not “prevent or significantly interfere” with a national bank’s authority to sell insurance. The Court did not leave the meaning of the phrase “prevent or significantly interfere” solely to the imagination. Instead, the Court placed that phrase within the context of several other preemption cases previously decided by the Supreme Court. In those cases, the Supreme Court said that state laws that unlawfully *encroach, destroy, hamper, or impair* the operation of a national bank are subject to preemption. Thus, when the phrase – *prevent or significantly interfere* is read in conjunction with the entire decision, it is clear that this “*Barnett Bank* preemption standard” is a *broad* and *flexible* one intended to override *any* state law that stands as “an obstacle” to the exercise of a national bank’s legitimate powers.<sup>4</sup>

In response to the discriminatory regulatory treatment of banks engaged in insurance sales by the States, Congress codified the decision in *Barnett Bank* in GLBA — including all favorably cited preemption standards — not just four words taken from the case. The relevant provisions of GLBA state:

In accordance with the *legal standards for preemption* set forth in the decision of the Supreme Court of the United States in *Barnett Bank of Marion County N.A. v. Nelson*, 517 U.S. 25 (1996), *no State may . . . prevent or significantly interfere with the ability of a depository institution . . . to engage . . . in any insurance sales, solicitation, or crossmarketing activity.*<sup>5</sup> (Emphasis added)

To preserve state insurance powers, Congress also provided thirteen “safe harbors” from preemption for state regulatory authority over bank insurance sales activities.<sup>6</sup> State laws that

---

<sup>2</sup> 15 U.S.C.S. § 6807

<sup>3</sup> Ass'n of Banks in Ins. v. Duryee, 270 F.3d 397, 405 (6th Cir. 2001).

<sup>4</sup> In *Association of Banks in Insurance (ABI) v. Duryee*, the Federal District Court of the 5th District of Ohio further explained that preemption under *Barnett Bank* is not limited to state laws that prohibit bank-affiliated insurance agencies from engaging in an authorized insurance agency activity, but also is warranted when the statute harms bank operations; increases a bank’s costs of operating; requires a bank to operate inefficiently; or places obstacles in front of banks – all principles it derived from the *Barnett Bank* case.

<sup>5</sup> 15 U.S.C.S. § 6701(d)(1).

<sup>6</sup> 15 U.S.C.S. § 6701(d)(2)(B).

imposed restrictions substantially the same as the safe harbors, *but not more restrictive*, are protected from federal preemption. Only two of the thirteen safe harbors relate to information sharing. One of these safe harbors relates to sharing *health information* and the other safe harbor relates to sharing *insurance information*.<sup>7</sup> Specifically, a state may impose restrictions that are substantially the same but no more burdensome than the following with respect to the sharing of *insurance information*:

(vi) Restrictions prohibiting the release of the *insurance information* of a customer (*defined* as information concerning the premiums, terms, and conditions of insurance coverage, including expiration dates and rates, and insurance claims of a customer contained in the records of the depository institution or an affiliate thereof) *to any person other than an officer, director, employee, agent, or affiliate of a depository institution, for the purpose of soliciting or selling insurance, without the express consent of the customer, other than a provision that prohibits . . . the release of information as otherwise authorized by State or Federal law*.<sup>8</sup> (Emphasis added)

As an initial matter, this is a narrow safe harbor that is related solely to *insurance information*. The Exposure Draft would impose information sharing limitations on depository institutions regarding categories of information much broader than *insurance information*. Moreover, the GLBA *explicitly authorizes* sharing nonpublic personal information under a joint marketing agreement *without an opt-out notice* and the safe harbor provision does not apply to the release of *insurance information* authorized by Federal law, which would include information released under a joint marketing agreement. This principle is also reiterated in Section 6701(d)(1):

[N]o State may, by statute, regulation, order, interpretation, or other action, *prevent or restrict a depository institution or an affiliate thereof* from engaging directly or indirectly, either by itself or in conjunction with an affiliate, or any other person, *in any activity authorized or permitted under this Act and the amendments made by this Act*.<sup>9</sup> (Emphasis added)

The word “Act” in Section 6701(d)(1) refers to the *entirety* of the Gramm-Leach-Bliley Act. Accordingly, given that depository institutions are permitted under the GLBA to share nonpublic personal information pursuant to a joint marketing agreement without providing consumer’s a right to opt-out, the current joint marketing provision (and likely other provisions) in the Exposure Draft are preempted with respect to depository institutions and their insurance affiliates.

## **II. Like Other NAIC Model Laws, the Exposure Draft Should Recognize the Unique Regulatory Framework Depository Institutions are Subject To**

Following enactment of GLBA, the NAIC recognized the need for action and established a Working Group to amend the model Unfair Trade Practices Act to recognize the GLBA

---

<sup>7</sup> 15 U.S.C.S. §§ 6701(d)(2)(B)(vi) & (vii).

<sup>8</sup> 15 U.S.C.S. § 6701(d)(2)(b)(vi).

<sup>9</sup> 15 U.S.C.S. § 6701(d)(1).

preemption standards. The working group's efforts were designed to ensure that any amendments to the model act that might later be adopted by a state were consistent with the preemption standards outlined in GLBA. The proceeding citations to the Unfair Trade Practices Act<sup>10</sup> evidence these efforts and specifically acknowledge that the safe harbors serve as a ceiling and not a floor with respect to state regulation of insurance sales by depository institutions:

GLBA provided 13 'safe harbors' from preemption for state regulatory authority over bank sales activities. State laws that imposed restrictions that are substantially the same as the safe harbors, but not more restrictive, were protected from federal preemption. 2000 Proc. 1st Quarter 985.

The proceeding citations to the Unfair Trade Practices Act also illustrate that the working group only addressed 11 of the 13 safe harbors in the amendments to the model Unfair Trade Practice Act as the remaining safe harbors were addressed in the current model laws the Working Group now seeks to amend:

During development of the 2001 amendments, regulators addressed 11 of the 13 safe harbors in the proposed amendments to the Unfair Trade Practices Act. They decided not to address the two safe harbors related to privacy, as the NAIC's privacy regulations adequately addressed privacy disclosures. 2001 Proc. 2nd Quarter 836.

The following drafting note to the Unfair Trade Practices Act was also specifically included to ensure that states adopted legislation that was consistent with the preemption standards outlined in GLBA:

The Gramm-Leach-Bliley Act contains two 'safe harbors' that relate to information sharing. Section 104(d)(2)(B)(vi) describes the circumstances surrounding the release of a customer's insurance information. Section 104(d)(2)(B)(vii) describes the circumstances surrounding the use of a customer's health information obtained from the insurance records of the customer. *If a state has adopted the NAIC's Privacy of Consumer Financial and Health Information Model Regulation, no further action is needed. If not, language implementing the two safe harbors should be considered.*

In short, after passage of the GLBA, the NAIC expended significant resources and time to ensure that model laws were consistent with the preemption standards outlined in the GLBA and *Barnett Bank*. We urge the Working Group to not unravel the NAIC's past efforts in this regard.

### **III. To Avoid Preemption Challenges, the Working Group Should Exempt Depository Institutions and their Affiliates from the Exposure Draft**

The entire framework for state regulation of bank-insurance activities is set forth in the GLBA. The NAIC and the states have been on notice since enactment of GLBA in November 1999 that

---

<sup>10</sup> NAIC Unfair Trade Practices Act, PC-880-1 & 880-2, available at, [https://content.naic.org/sites/default/files/inline-files/MDL-880\\_0.pdf](https://content.naic.org/sites/default/files/inline-files/MDL-880_0.pdf)

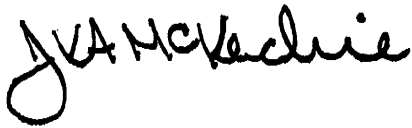
not only was *Barnett Bank* the law of the land, but that its application has been broadened to *all* depository institutions and their insurance affiliates. To date, the Working Group has not given adequate attention to these issues and as a result, has released an Exposure Draft that effectively amends the GLBA and unravels the NAIC's prior efforts in ensuring that state laws are consistent with GLBA preemption standards. For these reasons, we believe the Working Group should revise the Exposure Draft to exempt depository institutions and their affiliates. Specifically, we request that the Working Group add a new subsection "D" under Section 1 (titled Purpose and Scope) that states:

The obligations imposed by this Act shall not apply to depository institutions or affiliates of depository institutions that are subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.).

We have every confidence that the Working Group will adopt our recommended revisions in recognition of the unique regulatory framework depository institutions and their insurance affiliates are subject to.

Thank you for your consideration.

Respectfully,

A handwritten signature in black ink that reads "J. Kevin A. McKechnie". The signature is written in a cursive, flowing style.

J. Kevin A. McKechnie  
Executive Director

**July 28, 2023**

Chair Katie Johnson (VA)  
Vice Chair Cynthia Amann (MO)  
2023 NAIC Privacy Protections (H) Working Group  
NAIC Central Office  
1100 Walnut Street  
Suite 1500  
Kansas City, Missouri 64106

Sent via email to: [lalexander@naic.org](mailto:lalexander@naic.org)

**RE: Insurance Consumer Privacy Protection Draft Model Law #674 (Model #674)**

Dear Chair Johnson and Vice Chair Amann:

The Committee of Annuity Insurers (CAI or Committee)<sup>1</sup> appreciates the opportunity to submit the following comments to the 2023 NAIC Privacy Protections (H) Working Group (Working Group) on the exposure draft of Model #674 version 1.2 (published July 11, 2023) (the Revised Draft). We applaud the Working Group's continuing efforts on this complex and important issue and its commitment to continuing to work collaboratively over the coming months with consumer and industry stakeholders in order to craft effective and pragmatic enhancements to consumer privacy protections that are tailored to the insurance sector.

**OVERVIEW**

The CAI recognizes and appreciates the Working Group's efforts to respond to and reflect previous comments made by the CAI and others. The Revised Draft certainly represents a step in the right direction toward providing enhanced privacy protections to consumers in a way that is pragmatic and workable for licensees. That said, the CAI continues to have significant concerns regarding the Revised Draft, including issues we previously commented on as well as new issues arising from new language contained in the Revised Draft.

As revised, Model #674 would dramatically change the equilibrium that has been struck among insurance, banking and securities regulators regarding consumer privacy rights by placing much stricter limitations on insurance licensees' ability to process their consumers' data relative to the banking and securities sectors. This would put CAI members and all insurers at a competitive disadvantage in the broader marketplace for financial products, including by prohibiting their use of certain personal information even with the consumer's consent and reducing the ability of insurers to market products to consumers who may benefit from those products.

As you continue to work on the draft Model #674, we again urge you to be mindful of the balance between protecting consumers and enabling the smooth and efficient operation of insurance businesses that provide necessary and important financial protection and tools to those consumers. We also urge you to be mindful of the interplay between the various provisions of the Revised Draft and how they

---

<sup>1</sup> The Committee of Annuity Insurers is a coalition of life insurance companies that issue annuities. It was formed in 1981 to address legislative and regulatory issues relevant to the annuity industry and to participate in the development of public policy with respect to securities, state regulatory and tax issues affecting annuities. The CAI's current 31 member companies represent approximately 80% of the annuity business in the United States. More information is available at <https://www.annuity-insurers.org/>.

may result in conflicting approaches to the same issue and unintended outcomes. To assist stakeholders, including the CAI, in responding to the Working Group's ongoing efforts, we also request that the Working Group provide additional commentary on the Working Group's thinking and intended approach to issues under consideration in the Revised Draft.

Our comments below focus on several significant aspects of the Revised Draft that CAI members believe warrant particular attention in this regard.

## COMMENTS

### **1. The data minimization limitations, including consent requirements for marketing, would limit the ability of licensees to compete in the marketplace and innovate in the future.**

#### **a. Limiting licensees to processing personal information for only statutorily permitted purposes is the wrong approach.**

The Committee recognizes and appreciates the changes made to Section 4 on data minimization and Section 5 on sharing limitations to expressly allow certain marketing activities, including the ability to market non-insurance financial products and services without obtaining consumer consent. That said, the problematic overall approach taken by Model 674 does not appear to have changed.

Sections 4 (Data Minimization) and 5 (Sharing Limitations) would still limit the ability of insurance licensees to collect, process, retain, or share personal information collected in connection with providing an insurance product or service to a narrow list of statutorily defined circumstances. Collecting, using, or sharing any personal information that cannot be tied back to an "Insurance Transaction" would be an "additional activity" and would require consumer consent. Additionally, Section 5(A) appears to further limit the purposes for which personal information may be collected in connection with an "Insurance Transactions" to only when "necessary" to carry out certain defined purposes related to an "Insurance Transaction".

This approach continues to be overly restrictive, and would inhibit innovation and flexibility in the insurance marketplace. Sitting here today, neither regulators nor licensees can hope to accurately identify and quantify the full scope and variety of activities that licensees conduct as part of their businesses today, nor how their offerings will evolve in the future. Accordingly, any list of permissible "Insurance Transactions" and related purposes for processing personal information defined in Model 674 will inevitably be overly narrow as the market continues to develop. Additionally, fixing or updating the list would require legislative action on a state-by-state basis, an exceptionally difficult and slow process. Accordingly, this approach will inevitably hamstring the insurance industry, suppressing innovation and harming its ability to compete in the broader financial service marketplace.

*CAI Recommendations.* We request that licensees be permitted to collect, use and share personal information consistent with their privacy disclosures, without making artificial distinctions between an insurance transaction and "additional activities", subject to certain opt-out rights. Consent to collect, use and share personal information should not be required. Collection of personal information should still be minimized to that data that is reasonably necessary for the disclosed purposes for which the personal information is collected. This approach would be consistent with the approaches taken under the California Consumer Privacy Act and other existing and emerging US and international privacy laws.

#### **b. Licensees must be able to share privileged information with certain non-affiliated third parties.**

As drafted, Section 5(B) of the Revised Draft would require licensees to obtain consumer consent to share "privileged information" with any non-affiliated third party. "Privileged Information" is defined to include any personal information that relates to a claim for insurance benefit or any civil or criminal proceedings involving a consumer. There is no exception provided for sharing information with outside counsel, independent claims adjusters, or similar third parties. Licensees clearly need to be able to share information with such third parties in order to engage in normal day-to-day operations, including as necessary to pursue or protect their legal interests.

CAI Recommendations. Section 5(A) should be amended to provide that consent is not required where privileged information is shared with a third-party service provider. We suggest doing so through the addition of a new section that specifically permits licensees to share personal information with third-party service providers to the extent reasonably appropriate in connection with the services being provided.

**c. Clarify the limitation on third parties further sharing personal information in connection with additional activities.**

Section 5(C)(2)(a) appears intended to limit third parties who receive personal information in connection with providing additional activities from further sharing the information. However, as currently drafted this section would prohibit any “person” conducting additional activities from further sharing personal information, which would include licensees directly providing such additional activities. This would effectively prohibit licensees from using third-party service providers in connection with additional activities, even with consumer consent.

CAI Recommendations. This section should be clarified to refer to a “third party” instead of a “person”.

**d. Consumers should be empowered to decide how their personal information can be used and shared.**

Section 5(C)(2)(b) of the Revised Draft would prohibit any sharing of “Sensitive Personal Information” in connection with additional activities involving marketing a non-insurance or non-financial product or service. This appears to be a flat prohibition, regardless of consumer intent. Additionally, while this provision appears to only prohibit sharing the data, Section 6(C)(4) suggests it is meant to operate as a broader prohibition on even internal uses of Sensitive Personal Information for marketing of additional activities. Instead of empowering consumers to choose how their personal information is used and shared, this provision would make the decision for them. It would also prevent licensees from engaging in normal marketing practices that help them to effectively market beneficial products in a crowded and competitive market.

Similarly, Section 5(E) appears to be a broad prohibition on selling consumers’ Personal Information, regardless of consumer intent or consent.

CAI Recommendations. Processing or sharing personal information should never be flatly prohibited. Rather, consumers should be empowered to opt-out of the sharing of sensitive personal information or selling of personal information, subject to certain exceptions.

**2. Revise sections where consumer consent appears to be required for opt-out rights.**

The CAI appreciates that the Working Group has responded to previous comments made by the CAI and others by incorporating language in the Revised Draft that seems to move from a consent based approach to an opt-out approach for marketing and joint marketing activities. However, there are several sections of the Revised Draft that seem to cut against this approach and make it unclear as to whether some form of consent or authorization remains required.

For example, Section 5(A)(14) defines what licensees must do to engage in joint marketing, which states that consumers must be provided the right to “opt-out”. However, Section 5(A)(14)(c) appears to also require an “authorization” that complies with Section 6 (Consumer’s Consent). Requiring consent or authorization of any kind to engage in marketing is diametrically opposed to an “opt-out” approach. It is therefore unclear as currently drafted what is required for licensees to use personal information for marketing, and whether the law takes an opt-in or opt-out approach. The same issue exists in Section 5(A)(15) regarding what is required to engage in marketing.

Similarly, Section 6(A) seems to indicate that consumer consent could be required in connection with both opt-in and opt-out rights, stating “Where the consumer’s consent . . . is required by this Act, whether opt-in or opt-out, . . .” This language is self-contradictory. Any approach that requires consumer



consent or authorization is not an opt-out requirement, but rather an opt-in requirement. A similar issue exists in Section 6(B).

*CAI Recommendations.* The Revised Draft should be further revised to clarify that consent is not required in connection with marketing or joint marketing activities, and rather that an opt-out approach is being taken. At a minimum, subsections (c) should be deleted from both Sections 5(A)(14) and (15). Additionally, the reference to “whether opt-in or opt-out” should be deleted from Sections 6(A) and (B).

### **3. Clarify that de-identified information is not personal information and is excluded from the restrictions and requirement of Model 674.**

The Revised Draft includes conflicting language regarding how de-identified information is treated under Model 674 and causes confusion over the extent to which de-identified information is subject to regulation under Model 674. The Definition of “Personal Information” in Section 2(DD) clearly states that de-identified information is not personal information. We believe this reflects the Working Group’s intent, and is appropriate since the use of de-identified information does not pose privacy risks to consumers.

However, Section 5(D) appears to limit the ability of licensees to collect, process, retain, or share de-identified personal information to only “as necessary in connection with insurance transactions and additional activities”. This is incongruous and inconsistent with the definition of personal information, and would regulate de-identified data as a subset of personal information.

Similarly, several provisions in the Revised Draft would require that personal information be entirely deleted in various circumstances, without allowing for de-identification in lieu of deletion. For example, Section 7(C)(1) would mandate that personal information be “deleted” within 90 days of a determination that the personal information is no longer needed for certain specified purposes. The definition of “delete” in Section 2(M) states this means such data must be “permanently and completely eras[ed].” It does not allow for de-identification. Indeed, Section 7(C)(2) suggests that de-identification is only permissible where deletion is not feasible. This approach would lead to the incongruous result that the same de-identified information would be permissible for licensees to maintain if it was collected in a de-identified manner, but would be impermissible to keep if it was collected in an identifiable form and later de-identified. It is unclear what regulatory purposes this approach would serve.

*CAI Recommendations.* We request clarification that a licensee could de-identify personal information in lieu of deleting it, as such data would no longer be personal information. This could be accomplished by amending the definition of “delete” to allow for de-identification and by deleting Sections 5(D) and 7(C)2.

### **4. The requirements for enhanced third party oversight and contracting requirements would still adversely limit the ability of licensees to hire top service providers.**

The Revised Draft contains largely the same third party oversight provisions as previously proposed and continues to raise issues of significant concern. Section 3(B) would continue to require third-party service providers to agree to “abide by the provisions of this Act” and to require them to implement appropriate measures to “comply with the provisions of this Act”. As drafted, this appears to be an attempt to exercise long-arm jurisdiction over third-party service providers through contractual requirements that the licensee must impose. As we previously commented, many service providers will not be willing to agree to comply with a law that would not otherwise apply to them. In practice, these requirements would serve only to alienate quality service providers from serving the insurance sector, and limit the ability of licensees to assess and manage the privacy risks posed by third-party service providers. We reiterate our comments made on this issue in our previous comment letter dated April 3, 2023 and maintain that licensees should be empowered to pick the best vendor overall, not just the vendors willing to agree to certain contractual language.

Section 3(G) also carries over an additional issue from the previous draft of Model #674 by requiring that contracts with third-party services providers require that both the licensee and service provider must comply with consumer “directives”. As drafted, both parties would be prohibited from “collecting,

processing, retaining, or sharing the consumer's personal information in a manner inconsistent with the directive of the consumer", regardless of whether that directive goes beyond the consumer rights otherwise provided in Model # 674. This would be virtually impossible for licensees and service providers to comply with in practice, and would be extremely burdensome.

CAI Recommendation. Instead of applying a one-size-fits-all approach that will limit the ability of licensees to engage the best service providers in the market, Model #674 should be revised to take a risk-based approach. The CAI recommends that the Model require licensees to conduct appropriate due diligence and oversight of all third party service providers that process personal information, and require licensees to negotiate appropriate contractual protections based on the assessed risk of the service provider. The Model should not specify what those contractual protections would include beyond limiting the service providers' ability to use, share or disclose personal information for purposes other than providing the services and requiring the third party's cooperation when consumers exercise their rights to data correction and deletion.

Section 3(G) should be deleted. Alternatively, at minimum, Section 3(G) should be revised to clarify that parties must honor a consumer's decision to exercise rights provided under Model # 674, not comply broadly with any directive submitted by a consumer.

## **5. Key definitions need clarification and refinement.**

### **a. The definition of "consumer" should be clearly focused on personal information collected in connection with an insurance transaction.**

As currently drafted, the definition of a "consumer" in the Revised Draft is extremely broad, and would appear to include virtually any individual whose personal information a licensee collects. Section 2(I) currently defines "consumer" to include information on any individual "whose personal information is used, may be used, or has been used in connection with an insurance transaction. Including any individuals whose information could possibly be used ("may be used") in connection with an insurance transaction expands the definition significantly with no clear boundary. For example, this definition could be interpreted to apply to employee information, business partner information, and other information that is not actively collected in connection with an insurance transaction, since any such information could potentially be used in connection with an insurance transaction in the future. This drafting of the definition would seem to be at odds with other provisions of Model # 674, which are appropriately focused on protecting actual insurance customers rather than any personal information that happens to be collected by a licensee.

CAI Recommendations. The definition of "Consumer" should be aligned with the existing definition in Model # 672.

### **b. The definition of "personal information" should be clarified.**

As currently drafted, the definition of "personal information" under Section 2(DD) would be limited only to the specific types of personal information listed under Section 2(DD)(1). This drafting would appear to contrast to the apparent intent of the language otherwise included in Section 2(DD) defining personal information as "any individually identifiable information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to a consumer . . . ."

Additionally, there appears to be a typo in the definition, as it states that the definition applies to consumer information "that is by or on behalf of a licensee . . . ." A word appears to be missing from this phrase, and it is unclear what it is meant to convey.

CAI Recommendations. The definition of personal information should be revised and clarified, including to clearly indicate whether the list of items in Section 2(DD)(1) are meant to be an exclusive or illustrative list of what constitutes "personal information".

### **c. Define "additional activities".**

The concept of “additional activities” is central to the current Revised Draft of Model 674. However, this key term is not defined. Based on how it is used within the Revised Draft, it appears intended to include any activity that is not defined as an “Insurance Transaction”. To the extent the concept of “additional activities” is retained in future drafts, the term should be clearly defined. However, we reiterate that consent should not be required to collect or use information consistent with privacy disclosures made to consumers.

**d. Amend the definition of “personal information” to exclude “publicly available information”.**

Unlike NAIC Model #672 Section 4(T)(2)(b), which excludes publicly available information from the definition of “personal information” in a manner similar to other state privacy laws, the Revised Draft does not explicitly exclude “publicly available information” from its scope. Rather, it restricts or adds requirements to the use of “publicly available information” throughout the draft, such as in Section 3(C), which permits a licensee to share “publicly available information” with a third party service provider only to the extent necessary to provide the service requested by the consumer. Similarly, new language in Sections 12 and 13 would require consumers to submit verifiable requests to access the consumer’s personal and publicly available information in the possession of a licensee or its third-party service providers. Including “publicly available information” in this privacy law would be unprecedented, overly burdensome and detract from the purpose of privacy laws, which is to protect the privacy of private personal information.

CAI Recommendations. The scope of the requirements of the Revised Draft should be restricted to “personal information,” and “publicly available information” should be explicitly excluded from the definition of “personal information.” All references to “publicly available information” that impose additional restrictions or burdens on licensees should be deleted.

**e. Clarify the definition of an “insurance transaction”.**

As currently drafted, the definition of “insurance transaction” under Section 2(V) appears to contain language that would result in unintended consequences. The first sentence of the definition provides that an insurance transaction is any transaction “by or on behalf of a licensee and its affiliates” (emphasis added). As drafted, this would mean that any of the specific transactions listed in the definition that follow this phrase would only qualify as insurance transactions if they are provided by both the licensee and its affiliates; the same transaction provided just by the licensee would not qualify. We do not believe this is the intended meaning.

Additionally, Subsection 2(V)(7) appears intended to provide flexibility for licensees to process personal information for short-term transient uses. However, as drafted the provision appears to enact additional limitations on the ability of licensees to engage in common marketing practices that would otherwise be permissible under the Revised Draft. Additionally, it does not expressly state that it is referring to the short-term, transient use of personal information; it simply refers to “short-term, transient use.”

CAI Recommendations. The definition of “insurance transaction” should be reviewed and revised to clarify that an “insurance transaction” includes transactions or services provided by licensees or their affiliates, and to broadly permit short-term, transient uses of personal information.

**6. The limits on data retention in Section 7 should be revised to allow more flexibility.**

**a. Permitting retention of personal information only for the duration of an insurance transaction with the consumer should be modified to permit retention for any reasonable business purpose, as disclosed in the privacy notice.**

Revised Section 7(A)(1) would permit retention of personal information “as necessary” for “the performance of any insurance transaction with the consumer”, after which the data must be deleted.

However, a retention scheme that relies on transactions with consumers fails to allow licensees to retain personal information received from affiliates and other financial institutions for legitimate business purposes, such as joint marketing. For example, once a single joint marketing campaign has been completed and the personal information used in connection with that campaign is no longer strictly “necessary” for purposes of that campaign (an insurance transaction), a licensee would be required to delete that personal information even if it will just need to gather the information again in the future for additional or limited campaigns.

*CAI Recommendations.* This provision should be modified to allow licensees to retain personal information for any reasonable business purpose, and as disclosed in their privacy notice.

**b. An annual review of “all consumers’ personal information in its possession” is highly burdensome and should be changed to a review by category or type of personal information**

Revised Section 7(B) would require a licensee to annually review its data retention and “review all consumers’ personal information in its possession” to determine whether the purposes for which the personal information was retained still remain. As drafted, licensees would be required to review all of the actual consumer personal information in its possession, as opposed to conducting a broader assessment of the types and amounts of personal information it retains. The annual review of all consumers’ personal information in its possession is highly burdensome and unwarranted.

*CAI Recommendations.* Section 7(B) should be revised to clarify that the requirement is to annually review the type and amount of personal information in the licensee’s possession, not specific personal information.

**c. The 90-day period to completely delete a consumer’s personal information should be extended.**

Revised Section 7(C)(1) provides that once a licensee has determined that the consumers’ personal information is no longer needed, then the licensee shall completely delete all the consumers’ personal information within 90 days. We had previously commented that the 90-day time period to completely delete all personal information is too short and impractical, given the number of systems on which the personal information can be retained, including systems such as application, underwriting, operational, claims, distribution and other systems. Personal information will also be retained on backup systems, which present special issues and may be accessible only on a quarterly basis. Moreover, given the length of time that personal data must be retained, some consumer data may be in paper files that are archived and difficult to access.

The current version of the Model Law does not add flexibility on this point, other than to add new language that gives the commissioner the discretion to grant exceptions for good cause shown. Practical questions remain, however, regarding the severity of this 90-day requirement and regarding which commissioner would grant the exception, especially if one or more commissioners other than the commissioner in the insurer’s state of domicile can weigh in on this issue.

*CAI Recommendations.* Section 7(C)(1) should be revised to provide an annual deletion period, which would be more manageable and permit insurers to include deletion of personal information in their periodic cycles of system maintenance.

**d. The requirement to replace legacy systems within 10 years if they do not permit targeted disposal is highly prescriptive and costly without taking collateral consequences into account. Compensating controls should be permitted as an alternative to legacy system replacement.**

Section 7.C.(2) of the Revised Draft would require a licensee that cannot de-identify or delete consumers’ personal information from a system to replace the system within 10 years and to annually report to their domestic regulator on their progress in completing the project within those 10 years.

The commissioner has discretion to grant exceptions for good cause. Assuming the revised Model # 674 is ultimately adopted broadly, as currently drafted a licensee would be required to obtain an exception from each state commissioner in order to avoid having to migrate away from an existing legacy system.

The reality of migrating off of a legacy system in practice is extraordinarily complex, time consuming, and astronomically expensive. The process would easily take more than a decade to complete for some systems, and result in large costs that would necessarily be passed on to consumers. Part of the reason for this complexity and difficulty is that legacy systems are not stand-alone systems, but rather are deeply entrenched and enmeshed in licensees' information technology infrastructure. Migrating away from a legacy system would mean: (1) peeling back decades of custom and iterative software development and system design to disentangle the legacy system from the overall IT architecture; (2) migrating huge volumes of data to the new system in a way that transforms data from legacy formats to formats used by newer systems while ensuring consistency and fidelity in the data set; (3) integrating the new system with hundreds of other existing systems that interact with and depend on the existing legacy system to function; and (4) manage to complete all those tasks without disrupting ongoing business operations.

The task is enormous, comes with large amounts of operational and business interruption risk, and should not be taken lightly. We do not believe mandating such projects broadly across the insurance sector is an appropriate remedy to concerns about data minimization. Moreover, licensees are already subject to cybersecurity requirements, which require the adequate protection of personal information stored on legacy systems. Licensees have spent millions of dollars implementing compensating cybersecurity and privacy controls on their legacy systems, controls that are designed to appropriately protect consumer personal information held on such systems in satisfaction of existing NAIC and state standards. We do not believe mandating migration away from legacy systems is the appropriate remedy for addressing the cybersecurity risks of legacy systems.

CAI Recommendations. The proposed requirement to migrate away from legacy systems goes beyond the purview of privacy and what a privacy law is intended to accomplish. We respectfully submit that Model #674 is not the venue for addressing this issue. Instead, the CAI requests that this requirement be removed and that flexibility be provided to address legacy systems issues through the development and approval of appropriate compensating controls.

**7. The delivery of the notice of consumer privacy protection practices ("notice of privacy practices") in Section 8 should be revised and made more flexible.**

**a. The requirement to provide a notice of privacy practices when a licensee or third-party service provider first collects the personal information of a consumer is unworkable and should be revised.**

As currently drafted, revised Section 8(B)(1) would require a licensee to provide an initial notice of privacy practices to the consumer at the time the licensee, directly or through a third-party service provider, first collects, processes or shares the consumer's personal information in connection with an insurance transaction or additional activity. This provision is unworkable on several levels.

For example, assume the licensee is planning a digital marketing campaign and has obtained information about a consumer that does not include a street address. In such cases, how is the licensee going to send an initial notice of privacy practices to a consumer at the time the licensee first collects the consumer's information if the licensee has not obtained a mailing address for the consumer from the marketing agency? Note that Section 11(B)(3) would require the notice of privacy practices to be mailed to the individual at the time of collection.

Additionally, under the current language, the trigger for sending the notice of privacy practices is when the insurer receives the marketing leads from a third-party marketer, not when the licensee or its agent contacts the consumer. However, the licensee would not know whose information it is collecting until it receives the personal information, and therefore it would be impossible to comply with the

requirement to provide notice at the time the data is collected. Additionally, requiring every licensee that would market to a consumer to deliver a privacy notice would create a deluge of privacy notices to consumers that would render the notices ineffective and annoying.

*CAI Recommendations.* A more effective and relevant approach would be to revise Section 8(B)(1) so the sending of the notice of privacy practices was triggered when the licensee is first in direct contact with a consumer and can obtain the information necessary to send the privacy practices notice.

**b. The requirement on when to send a notice of privacy practices to a beneficiary should be clarified.**

New language in revised Section 8(B)(1) states that the term “consumer” includes a third-party claimant or beneficiary in connection with a claim under an insurance policy. However, there is ambiguity regarding when the initial notice of privacy practices must be sent to third-party claimants and beneficiaries. Often, an insurer licensee first collects a beneficiary’s name and possibly contact information at the time the insured applies for an insurance policy or contract. But the actual processing of a claim likely will occur much later.

*CAI Recommendations.* The Committee requests that Section 8(B)(1) be revised to clarify that a notice of privacy practices must only be delivered to beneficiaries at the time a claim is filed with the licensee.

**8. The requirement that the notice of privacy practices list the persons who received the consumer’s personal information should be deleted. In the same vein, consumers should not be given the right, in the notice of privacy rights, to obtain the identification of all persons who have received the consumer’s personal information.**

Revised Section 9(A)(5) continues to require that the notice of privacy practices state that a consumer may obtain a list of persons with whom the licensee or its third-party service provider has shared the consumer’s personal information in the three previous calendar years. Because the term “person” is defined to include individuals, this would require licensees to track and maintain a list of every individual, internal or external, that processes a particular individual’s personal information. We commented in our previous letter that this provision would be extremely costly, onerous and difficult to manage, while providing the consumer with little, if any, benefit.

Similarly, new Section 10(B)(e) would require a licensee to send a privacy rights notice to each consumer with whom the licensee has an ongoing relationship, giving the consumer the right to obtain “the identification” of all persons who have received the consumer’s personal information in the past three years. As drafted, this requirement would be extremely burdensome, as noted above, and serve no clear purpose.

*CAI Recommendations.* The Committee reiterates its previous request that Section 9(A)(5) be generalized so that the licensee would be required to give an indication of the categories of third parties with whom the consumer’s personal information was shared, not the names of individuals.

The Committee also requests that Section 10(B)(e) be generalized to provide notice of the types or categories of third parties with whom a consumer’s personal information has been shared.

**9. The delivery requirements for the notice of privacy practices and the notice of privacy rights should be symmetrical.**

Revised Section 8(C) requires that the notice of privacy practices be delivered only when the privacy protection practices of the licensee change. But new Section 10(C) requires that the notice of privacy rights be provided to the consumer at least once every year, which in many cases would require the notice to be physically mailed. This new requirement would be costly, would be inconsistent with the revised approach that Congress has taken to delivery of privacy notices, and would be of limited utility

to the consumer, especially since the notice of privacy rights would be posted on the licensee's website and always available.

CAI Recommendations. The Committee requests that the annual delivery requirement for the notice of privacy rights and the requirement for delivery of updated notice of privacy practices be revised to allow that website posting of the notices satisfies the requirements for delivery of both the notice of privacy practices and the notice of privacy rights.

**10. Delivery of initial notices required by the Act should be more flexible.**

While the Revised Draft has added some flexibility for delivering notices required by the Act, it would still generally require notices to be mailed in hardcopy as the default approach. This is out of step with a modern approach to delivering notices. We reiterate our previous comments on this issue.

CAI Recommendations. The Committee requests that further flexibility be provided to allow licensees to send initial notices by default in the way that the licensee generally engages with that consumer. This approach, consistent with the approach taken in the CCPA, would allow a consumer who frequently uses the licensee's website to receive the initial privacy notices electronically, unless the consumer requests delivery in another way.

We want to express our deep appreciation for the opportunity to comment on draft Model #674, and we hope that you find these comments helpful at this stage. Please do not hesitate to contact us if you have any questions.

Sincerely,

**For The Committee of Annuity Insurers**

Eversheds Sutherland (US) LLP

By:



Stephen E. Roth  
Mary Jane Wilson-Bilik  
Alexander F. L. Sand  
Eversheds Sutherland (US) LLP



Independent Insurance Agents  
& Brokers of America.

July 24, 2023

Katie Johnson  
Chair  
Privacy Protections Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106-2197

*Re: Draft Insurance Consumer Privacy Protections Model Law, Version 1.2*

Dear Chair Johnson:

On behalf of the Independent Insurance Agents and Brokers of America (IIABA), the largest insurance agent and broker organization in the country, I write to offer our association's comments and concerns regarding the latest draft of the *Insurance Consumer Privacy Protections Model Law (Version 1.2)*. Our members are the industry constituency that would be most impacted by this proposal, and we appreciate having the opportunity to submit these comments.

### **Comments and Observations**

IIABA is incredibly troubled by the proposal and would oppose legislation of this nature if ultimately introduced and considered by state policymakers. We recognize that modest revisions have been made in this second version, but those improvements are on the margins and fail to address a myriad of more significant threshold considerations and questions.

The latest draft remains inherently flawed and misses the mark. It would inappropriately restrict how and when data may be used and retained by licensees, impose unrealistic marketing restrictions, force small licensees to unreasonably police third-party service providers, expand privacy notice obligations in unnecessary ways, subject main street insurance agents to mandates that states have reserved only for large entities, and establish a range of other burdensome and unprecedented requirements. We cited numerous problems and suggested revisions in our April 3 correspondence and in numerous meetings, and those comments largely remain relevant vis-à-vis the updated draft.

The NAIC's Summer National Meeting will begin in less than three weeks, and we urge the working group and other regulators to use that time together to assess and discuss what the NAIC hopes to achieve with regard to privacy and what it can realistically accomplish. The



working group has elected to draft a new model law that would completely replace the existing privacy framework, but it is still unclear to most observers what problems and regulatory gaps the drafters see in the current privacy framework. It is similarly unclear why such a sweeping new proposal is necessary, beneficial, or likely to be adopted by state legislatures. There are other credible, helpful, and timely actions that the working group could pursue in lieu of a full-blown rewriting of privacy law, but we do not believe the current proposal is viable from a substantive or political perspective. The problems with the current approach are foundational and fundamental, and they cannot be cured with modest revisions or wordsmithing.

As the working group and other regulators consider how to move forward, we would also note the following:

- The working group has proposed a dramatic restructuring of privacy law that would uniquely target the insurance industry and create mandates more onerous and restrictive than those that apply to other industries, and it has done so without explaining its reasoning or examining the marketplace ramifications of such a proposal. This draft would create unwarranted burdens for the industry, hinder our ability to serve consumers, and have particularly adverse effects on small licensees and the independent agent system.
- Thirteen states, which represent over 41% of the country's population, have enacted comprehensive privacy measures or passed them through their legislatures, and the new draft directly conflicts with these recently adopted laws. This recent legislative activity offers insight into the current perspective of many state policymakers and highlights the fact that the NAIC proposal is unnecessary and out of the mainstream. It also suggests there is little interest in a model law that treats the insurance industry in uniquely and unduly restrictive ways. State legislators attending last week's National Council of Insurance Legislators meeting also commented publicly and suggested that the NAIC proposal would be poorly received by state legislatures.
- The working group has also not publicly discussed the manner in which the draft would considerably distort the marketplace and create an unlevel playing field among marketplace competitors. Certain federal laws, including the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, already impose privacy-related requirements on insurance and other financial services providers, and these laws affect and restrict the types of requirements states may impose. As a result of these existing federal statutes, the NAIC draft would create an uneven playing field, with some competitors being subject to its requirements and others being largely exempt from them as result of this preemption.
- Supreme Court decisions over the last dozen years have altered and expanded the manner in which commercial speech is protected by the First Amendment, and the draft has constitutional implications that have not been examined. The Supreme Court has indicated that the creation and dissemination of information is speech under the First Amendment and that marketing is a form of commercial speech. This means the proposed restrictions on the use and sharing of information would at least need to survive the intermediate level of First Amendment scrutiny, and these recent decisions also suggest that content-based and viewpoint-based restrictions on commercial speech could be subject to the higher strict scrutiny standard and almost certainly found unconstitutional.

## Next Steps

IIABA, like other industry stakeholders and business groups, does not believe the complete displacement of the existing privacy framework and the development of an entirely new privacy regime are warranted, appropriate, or beneficial. Sweeping and disruptive changes in state insurance codes are not needed, and regulators should instead focus on addressing marketplace problems and regulatory gaps. Regulators should also consider whether there are helpful changes or new elements (i.e. a modified version of the provisions contained in Article IV of the proposal) that could be blended with the existing statutory framework.

We urge the working group, its parent committee, and commissioner-level regulators in the coming weeks (including during your time at the Summer National Meeting) to consider what the NAIC hopes to accomplish with regard to privacy regulation, to consider alternative approaches in its privacy work, and to identify reasonable objectives. Adopting a narrower and more reasonable focus is not only more appropriate, but it would also significantly increase the likelihood that any final work product would (1) be approved by the NAIC in the aggressive timeframe that has been proposed and (2) be considered and adopted by state legislatures. We will, of course, continue to participate in your model development process, if that is the path that the NAIC chooses to take, but it is our sincere hope that the working group will embrace a slight but meaningful change in direction.

## Conclusion

IIABA appreciates having the opportunity to submit these comments. We are happy to assist the working group's consideration of these issues in any way it deems appropriate. Please feel free to contact me at 202-302-1607 or via email at [wes.bissett@iiaba.net](mailto:wes.bissett@iiaba.net) with any questions or if we can assist in any manner.

Very truly yours,



Wesley Bissett  
Senior Counsel, Government Affairs