ACLI Comments

Roberta B. Meyer
Vice President & Associate General Counsel

May 8, 2017

The Honorable Raymond G. Farmer, Chair
The Honorable Elizabeth Kelleher Dwyer, Vice Chair
Cybersecurity Working Group
NAIC Central Office
1100 Walnut, Suite 1500
Kansas City, MO 64106-2197

Attn: Sara Robben, Statistical Advisor
VIA Electronic Mail: srobben@naic.org

Re: Proposed NAIC Insurance Data Security Model Law – Version 4

Dear Director Farmer and Superintendent Dwyer:

ACLI is writing to provide initial comments on Version 4 of the proposed Insurance Data Security Model Law ("Model Law"). ACLI commends the Cybersecurity Working Group ("Working Group") for its efforts, reflected in Version 4, to develop a model law that provides risk-based security standards and the opportunity for necessary uniformity and consistency in security standards across the country. ACLI will follow up shortly with a more detailed letter outlining some technical concerns. However, ACLI believes Version 4 reflects significant and appreciated improvements over previous drafts of the proposed Model Law.

As stated previously, ACLI strongly concurs with remarks made during the 4/9/17 Working Group meeting relating to the need for uniform, risk-based security standards from state to state. As more states adopt enhanced security requirements, as anticipated, the need for uniformity will become increasingly important. Uniform, risk-based security standards will enhance level protection of consumers' personal information across the country, and will make it possible for insurance licensees to effectively protect the security of that information and the information systems on which the information is stored.

As indicated above, ACLI plans to provide the Working Group specific comments relating to some technical concerns and suggested modifications to Version 4. The concerns generally relate to the Model Act's intent to create exclusive security standards within the enacting state, some of the notice requirements and the underlying definition of "Cybersecurity Event," the effective date, and other technical matters.

Again, ACLI acknowledges and appreciates the positive movement reflected in Version 4 that we believe will lead to a Model Law that will benefit consumers as well as insurance licensees. ACLI thanks the Working Group for the opportunity to submit these comments and its continued consideration of our views.

Sincerely,

Roberta B. Meyer

American Council of Life Insurers
101 Constitution Avenue, NW, Washington, DC 20001-2133
(202) 624-2184 t (866) 953-4096 f robbiemeyer@acli.com
www.acli.com

AIA Comments

Section 1. Purpose and Intent

A. Cyber threats have evolved since the adoption of the Gramm-Leach-Bliley Act (GLBA) and will continue to evolve as our society becomes increasingly interconnected, bad actors adapt to new technology and defense measures, and industry adjusts its resiliency efforts. As such this Regulation builds upon the Standards for Safeguarding Customer Information Regulation, which implements GLBA, and identifies additional risk-based regulatory expectations for a defined set of Personally Identifiable Information.

B. The Standards for Safeguarding Customer Information Regulation identifies basic requirements that covered entities must meet for a broadly defined universe of nonpublic personal information. This Regulation compliments and expands on the existing Standards for Safeguarding Customer Information Regulation for a defined set of nonpublic personal information, which we have defined as Personally Identifiable Information.

C. Harmonization, coordination and uniformity are important foundations to protect consumers and efficiently regulate cyber threats that cross state and global borders.

[Drafting Note: States that have not adopted the Standards for Safeguarding Customer Information Model Regulation should consider deleting paragraph B and substituting the following subparagraph A language: Cyber threats have evolved since the adoption of the Gramm-Leach-Bliley Act (GLBA) and will continue to evolve as our society becomes increasingly interconnected, bad actors adapt to new technology and defense measures, and industry adjusts its resiliency efforts. As such this Regulation builds upon the principles established by the GLBA and identifies additional risk-based regulatory expectations for a defined set of Personally Identifiable Information.]

Section 2. Definitions

For purposes of this Regulation, the following definitions shall apply:

A. Affiliate means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

B. Authorized User means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

C. Covered Entity means any Person operating under or required to operate under a license, third-party administrator registration, or certificate of authority under the Insurance Law of this State. A Covered Entity shall not include: a purchasing group, a risk retention group, entities operating under a limited lines producer license, accredited or certified reinsurers, charitable annuity societies, an unauthorized insurer as defined by [cite state surplus lines law], or a licensed individual.

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

E. Personally Identifiable Information shall mean all electronic information that is not Publicly Available Information and is:

(1) Any information concerning a resident of this state which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number in combination with any security code, access code or password that would permit access to an individual's financial account, or (iv) biometric records; and

(2) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a resident of this state and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

F. Penetration Testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

G. Person means any natural person or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

H. Publicly Available Information means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

I. Risk Assessment means the risk assessment that each Covered Entity is required to conduct under Section 10 of this Regulation.

J. Risk-Based Authentication means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

K. Security Incident means an act or attempt to gain unauthorized access to or to disrupt or misuse an Information System or Personally Identifiable Information stored on such Information System, that is reasonably likely to (i) cause identity theft or fraudulent transactions on financial accounts of the individual's to whom the Personally Identifiable Information relates, or (ii) result in a material adverse impact to the business operations or security of the Covered Entity.

L. Senior Officer(s) means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, Information Systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Regulation.

M. Third Party Service Provider(s) means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Personally Identifiable Information through its provision of services to the Covered Entity.

Section 3. Cybersecurity Program

A. Each Covered Entity shall maintain a cybersecurity program designed to protect the security, confidentiality, integrity and availability of the Covered Entity's Information Systems.

B. The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

1. identify and assess internal and external cybersecurity risks that may threaten the security, confidentiality, or integrity of Personally Identifiable Information stored on the Covered Entity's Information Systems;
2. use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Personally Identifiable Information stored on those Information Systems, from unauthorized access, use, or other malicious acts;
3. detect Security Incidents;
4. respond to detected Security Incidents to mitigate any negative effects;
5. recover from Security Incidents and restore normal operations and services; and
6. fulfill applicable regulatory reporting obligations.

C. A Covered Entity may meet the requirement(s) of this Section by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Section, as applicable to the Covered Entity.

Section 4. Cybersecurity Policy

Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer, the Covered Entity's board of directors (or an appropriate committee thereof), or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Personally Identifiable Information stored on those Information Systems. The polic(ies) shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

1. information security;
2. data governance and classification;
3. asset inventory and device management;
4. access controls and identity management;
5. business continuity and disaster recovery planning and resources;
6. systems operations and availability concerns;
7. systems and network security;
8. systems and network monitoring;
9. systems and application development and quality assurance;
10. physical security and environmental controls;
11. customer data privacy;
12. vendor and Third Party Service Provider management;
13. risk assessment; and
14. incident response.

Section 5. Chief Information Security Officer

A. Each Covered Entity shall designate a qualified individual responsible for overseeing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Regulation, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:
    1. retain responsibility for compliance with this Regulation;
    2. as applicable, designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and
    3. as applicable, require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Regulation.

B. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:
    1. the confidentiality of Personally Identifiable Information and the integrity and security of the Covered Entity's Information Systems;
    2. the Covered Entity's cybersecurity policies and procedures;
    3. material cybersecurity risks to the Covered Entity;
    4. overall effectiveness of the Covered Entity's cybersecurity program; and
    5. material Security Incidents involving the Covered Entity during the time period addressed by the report.

Section 6. Penetration Testing and Vulnerability Assessments

The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

1. annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and
2. bi-annual vulnerability assessments, including any systemic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity

vulnerabilities in the Covered Entity's Information Systems based on Risk Assessment.

Section 7. Audit Trail

A. Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment, include audit trails designed to detect Security Incidents that have materially harmed any material part of the normal operations of the Covered Entity.
B. Each Covered Entity shall maintain records required by this section for not fewer than one year.

Section 8. Access Privileges

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Personally Identifiable Information and shall periodically review such access privileges.

Section 9. Application Security

A. Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

B. All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

Section 10. Risk Assessment

A. Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Regulation. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Personally Identifiable Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Personally Identifiable Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Personally Identifiable Information and Information Systems.

B. The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

1. criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;
2. criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Personally Identifiable Information, including the adequacy of existing controls in the context of identified risks; and
3. requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

Section 11. Cybersecurity Personnel and Intelligence

A. In addition to the requirements set forth in Section 5, each Covered Entity shall:
   1. Utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risk and to perform or oversee the performance of the core cybersecurity functions specified in Section 3(B)1-6 of this Regulation;
   2. Provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and
   3. Verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

B. A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Regulation, subject to the requirements set forth in Section 12.

Section 12. Third Party Service Provider Security Policy

A. Each Covered Entity shall implement written policies and procedures designed to protect the security of Information Systems and Personally Identifiable Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:
   1. the identification and risk assessment of Third Party Service Providers;
   2. minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;
   3. due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Services Providers; and
   4. periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

B. Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:
   1. the Third Party Service Provider's policies and procedures for access controls,

including authentication as set forth in Section 13 of this Regulation, to limit access to relevant Information Systems and Personally Identifiable Information;

2. the Third Party Service Provider's policies and procedures for use of controls such as industry accepted cryptographic technology as set forth in Section 16 of this Regulation;

3. notice to be provided to the Covered Entity in the event of a Security Incident directly impacting the Covered Entity's Information System or the Covered Entity's Personally Identifiable Information being held by the Third Party Service Provider; and

4. representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Personally Identifiable Information.

C. An agent, employee, representative or designee of the Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Regulation.

D. A Covered Entity that interacts with a Third Party Service Provider that is also an exempt Covered Entity under Section 19 of this Regulation is permitted to rely on the exemption notice when assessing the risks presented by such third party.

Section 13. Authentication

A. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include multi-factor authentication or Risk-Based Authentication, to protect against unauthorized access to Personally Identifiable Information or Information Systems.

B. Multi-factor authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Section 14. Limitations on Data Retention

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Personally Identifiable Information as defined by this Regulation that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or Regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Section 15. Training and Monitoring

As part of its cybersecurity program, each Covered Entity shall:

A. implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Personally Identifiable Information by such Authorized Users.
B. provide cybersecurity awareness training for personnel that is updated, as necessary, to reflect risks identified by the Covered Entity in its Risk Assessment. The personnel to which the training is directed, as well as the type and frequency of training should also be based on the Covered Entity's Risk Assessment.

Section 16. Encryption of Personally Identifiable Information

A. As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, if deemed necessary by its Risk Assessment, to protect Personally Identifiable Information held or transmitted by the Covered Entity both in transit over external networks and stored on a laptop computer or other portable computing or storage device or media.

1. To the extent a Covered Entity determines, based on its Risk Assessment, that encryption of Personally Identifiable Information in transit over external networks is infeasible, the Covered Entity may instead secure such Personally Identifiable Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

2. To the extent a Covered Entity determines, based on its Risk Assessment, that encryption of Personally Identifiable Information stored on a laptop computer or other portable computing or storage device or media is infeasible, the Covered Entity may instead secure such Personally Identifiable Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

B. To the extent that a Covered Entity is utilizing compensating controls under (A) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

Section 17. Incident Response Plan

A. As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Security Incident materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

B. Such incident response plan shall address the following areas:

1. the internal processes for responding to a Security Incident;
2. the goals of the incident response plan;
3. the definition of clear roles, responsibilities and levels of decision-making authority;
4. external and internal communications and information sharing;

5. identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
6. documentation and reporting regarding Security Incidents and related incident response activities; and
7. the evaluation and revision as necessary of the incident response plan following a Security Incident.

Section 18. Notices to the Commissioner

A Covered Entity must notify the Commissioner as soon as reasonably practicable after determining there has been a breach as defined by [Stat. Reference] that will impact 500 or more residents of this state.

Section 19. Confidentiality and Exemption from Disclosure

The Department of Insurance will take appropriate steps to secure information provided to the Department by a Covered Entity under this Regulation in a manner that is commensurate to the risk that disclosure of such information poses and consistent with the requirements of this Regulation. Further, if any information submitted by a Covered Entity under this Regulation is (1) determined to be a trade secret which if disclosed would cause substantial injury to the competitive position of the Covered Entity; (2) compiled for law enforcement proceedings; or (3) information which, if disclosed, would jeopardize the capacity of the Covered Entity to guarantee the security of its information technology assets the Department shall presume the information is confidential unless there is compelling evidence that disclosure is in the best interest of the public and will not jeopardize the capacity of the Covered Entity to protect the security of Personally Identifiable Information or Information Systems or cause substantial injury to the competitive position of the Covered Entity.

Section 20. Exemptions

A. Each Covered Entity with:
1. Fewer than 10 employees (including any independent contractors) located in this [state] or responsible for the insurance business of the Covered Entity, or
2. Less than $5,000,000 in gross annual revenue in each of the last three fiscal years from [state] insurance business operations of the Covered Entity, or
3. Less than $10,000,000 in year-end total assets, calculated in accordance with general accepted accounting principles

shall be exempt from the requirements of Sections 5, 6, 7, 9, 11, 13,15, 16 and 17 of this Regulation.

B. An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Regulation and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

C. A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Personally Identifiable Information shall be exempt from the requirements of sections 3, 4, 5, 6, 7, 8, 9, 11, 13, 15, 16 and 17 of this Regulation.

D. A Covered Entity that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Personally Identifiable Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 5, 6, 7, 9, 11, 13,15, 16 and 17 of this Regulation.

E. A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption within 30 days of the determination that the Covered Entity is exempt.

F. In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Regulation.

Section 21. Effective Date

This Regulation shall be effective on [insert date]

Section 22. Transitional Periods

A. Covered Entities shall have 180 days from the effective date of this Regulation to comply with the requirements set forth in this Regulation, except as otherwise specified.
B. The following provisions shall include additional transitional periods. Covered Entities shall have
    1. One year from the effective date of this Regulation to comply with the requirements of Sections 5(B), 6, 13, and 15(b).
    2. Eighteen months from the effective date of this Regulation to comply with the requirements of Sections 7, 9, 14, 15a, and 16.
    3. Two years from the effective date of this Regulation to comply with the requirements of section 12 of this Regulation.

Section 23. Severability

If any provision of this Regulation or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Regulation or the application thereof to other Persons or circumstances.

ALTA Comments

Sara – We have been busy hosting one of our major meetings, so I have not had time to dig deep into the latest model with our members. I wanted to just get you some first blush thoughts ahead of the call.

Definition of Cybersecurity Event is Overly Broad

The model defines a Cybersecurity Event as, *"Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System."*

While this is very close to the NY regulation, it does not contain the important qualification in section 500.17 which limits notice to those that have a reasonable likelihood of materially harming the licensee or an insured.

Our concern would be that need to report even unsuccessful attempts to gain entry could be burdensome on both the licensee and the department. It is not unusual for a company to receive upwards of hundreds of unsuccessful probes and scans a day. These probes would seem to be reportable even thought they were blocked and do not threaten the security of licensee's system or Nonpublic Information. The burden could be increased even more if the licensee must report unsuccessful attempts on each Third-Party Service Provider.

We suggest revising the definition to read: " *Any act or attempt, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System that actually or imminently jeopardizes the confidentiality, integrity, or availability of systems or networks, or Nonpublic Information and is likely to result in substantial harm to a consumer and resident of this state or a Licensee*".

Remove "and others" from definition of Consumer
The term Consumer is defined as*, "an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, certificate holders* ***and others*** *who is a resident of this state and whose Nonpublic Information is in a Licensee's possession, custody or control."*
While we support the limitation of the definition to state residents, we are concerned that the the phrase "and others" makes this definition ambiguous. It appears that, a individual need not be an insurance customer at all but only a state resident whose NPI is in the "possession, custody or control of a licensee" or a third-party servicer. We believe the definition should be limited to actual or prospective customers of the licensee.

Definition of Information System:

The definition of "Information System" is overbroad and should be tailored to the insurance industry. We propose that the term "Information System" should read: "Information System means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic Nonpublic Information as it relates to consumers or Nonpublic confidential business information of the licensee.".

Thanks,

Steve Gottheim
Senior Counsel
American Land Title Association
202.261.2943 direct

California DOI Comments

DEPARTMENT OF INSURANCE
Government Law Bureau
300 Capitol Mall, 16th Floor
Sacramento, CA 95814

Damon Diederich
Attorney / Assistant Privacy Officer
TEL: (916) 492-3567
E-Mail: diederichd@insurance.ca.gov
www.insurance.ca.gov

April 17, 2017

VIA ELECTRONIC MAIL

Director Raymond Farmer
NAIC Cybersecurity (EX) Working Group
1100 Walnut Street, Ste. 1500
Kansas City, MO 64106

Attn: Sara Robben, Statistical Advisor
srobben@naic.org

SUBJECT: Insurance Data Security Model Law -
New York Cybersecurity Regulations

Dear Director Farmer:

During the recent Cybersecurity Working Group meeting in Denver on April 9, Superintendent Maria Vullo of New York provided an overview of cybersecurity regulations recently adopted by New York (23 NYCRR 500, *et seq.*). After acknowledging the lack of consensus around the current draft Data Security Model Law, you invited the Working Group to consider redirecting its efforts towards a focus on risk-based security requirements, as opposed to breach notice requirements. As part of this effort, it was proposed that the Working Group use New York's framework as the basis for discussions concerning a new draft of the NAIC Insurance Data Security Model Law. California supports use of the New York regulations as the starting point for creating minimum standards governing insurer risk governance.

The New York regulations outline a comprehensive, yet scalable approach to corporate risk governance. California believes that the New York regulations are a good foundation for minimum insurer cybersecurity standards, as the regulations highlight current best practices, including periodic risk assessments, penetration testing, access control, multi-factor authentication, and encryption. As a baseline for state data security standards, California agrees with Superintendent Vullo that the New York regulations will represent a significant improvement over Gramm-Leach-Bliley and older standards upon which they are intended to build.

While California supports use of the New York regulations as minimum standards for risk governance, California regulators feel it important to stress that Working Group membership must consider the regulations in their state-specific context when adapting them into the NAIC Model Law. The regulations will need to be altered by NAIC membership when adapting them to the regulatory challenges faced by each individual member. To be clear: California supports the New York framework only insofar as the Working Group pursues the adoption of minimum, rather than maximum, national cybersecurity standards for insurers and other insurance licensees.

Please contact me if you have any questions.

Thank you for your consideration.

Sincerely,

Damon Diederich
Attorney / Assistant Privacy Officer

CC: Susan Bernard, CDI
Bryant Henley, CDI
Susan Stapp, CDI

CEJ Comments

CENTER for ECONOMIC JUSTICE | FAIR ACCESS FAIR TREATMENT

Comments of the Center for Economic Justice

To the NAIC Cybersecurity Working Group

On Version 4 of the Insurance Data Security Model Law

May 8, 2017

CEJ submits the following comments on version 4 of the proposed Insurance Data Security Model Law.

General Comments

The latest version of the model law has rewarded insurers and producers for their refusal to agree to, or compromise on essential personal consumer data protections, accountability or data breach obligations by eliminating anything industry has opposed. The current model has literally nothing for the consumers whose personal data insurers are mining, using, storing and selling. The current model provides zero accountability of licensees to consumers for data security or of insurance regulators to consumers for enforcement of the data security requirements. The current model provides no penalties for bad outcomes for consumers and is generally an exercise in Licensee self-regulation. The model borrows from the New York Cybersecurity Regulation, but omits that regulation's reliance on strong consumer data breach notification requirements in other New York law and creates harm triggers not found in the New York version.

Even assuming that consumer data protection and data breach notification and response issues will be addressed in a subsequent, companion model, version 4 requires, at a minimum, additions to create accountability to consumers of licensee data security practices and outcomes and for regulators' oversight and enforcement of licensee requirements. Towards this end, a section or sections are needed for independent assessment and publication of licensees' compliance with data security procedures. This information is essential to enable consumers to consider a licensee's data security procedures and competence when selecting a licensee with whom to do business.

Independent Assessment of Licensee Compliance and Data Security Program Effectiveness

Regulators and insurers urge consumers to select insurance providers based on their financial strength and consumer outcome performance in addition to shopping based on price. But, we are in an era where insurers mine, use and maintain vast amounts of consumers' personal information in the sale and administration of insurance products. Surely, one area for innovation – as well as fundamental accountability to consumers – is to develop a public grading system for licensees' protection of consumers' personal information to allow consumers to incorporate personal data protection into the decision to purchase from and do business with a licensee.

One likely response to this recommendation from insurers is that regulators will enforce the requirements of the model law and consumers are protected by that enforcement. There are several fatal problems with this rationale. First, the proposed model is largely a self-regulatory model with broad and vague requirements. For example, section 4A – Implementation of an Information Security Program

> Commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control, each Licensee shall develop, implement, and maintain a comprehensive risk-focused written Information Security Program that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information. The Licensee shall document, on an annual basis, compliance with its Information Security Program. The Licensee shall make this documentation available to the Commissioner upon request

Per this foundational provision of the model, the licensee determines what its risk is, designs a program based on its evaluation of its risk and evaluates itself on its performance in complying with a program it designed for a risk it assessed.

Second, the model includes procedural requirements only, presumably based on the belief that good policies and procedures will produce good (or better) outcomes, but no provisions based on actual data security program results. While such an approach is necessary for financial regulation since there are too few bad outcomes (financial failures) to create a statistically-valid methodology for correlating certain policies and procedures with certain outcomes, that is not the case with data security program. Problems with data security programs – small and large, data breaches and data security program failures not resulting in a breach – are numerous enough to measure the outcomes of data security programs. Stated differently, the model should require reporting and publication of data security program successes and failures and include monitoring and assessment of outcomes to inform and improve policies and procedures.

Third, in addition to the model creating no accountability to consumers from licensees, the model also contains no accountability to consumers from regulators charged with enforcing the vague provisions of the model. There are no provisions in the model – except for the

optional (!) rulemaking provision – to generate more specific regulatory practices for consistency across states. Not only is there no mechanism for regulators to agree upon the size and complexity of a Licensee or the nature and scope of a Licensee's activities or the sensitivity of the Licensee's Nonpublic Information or what the risk-focus of a Licensee should be, there is no accountability to consumers of regulators' performance. Consumer concern with uneven enforcement across the states is justified by uneven use of state-prescribed accounting practices and many states' commitment to insurance as an economic development strategy for their state.

Based on this analysis, we urge the working group to add provisions to the model allowing for independent assessment and publication of Licensees' performance meeting the data security requirements of the model. The independent assessment would grade the Licensee as not-meeting-requirements, meeting-requirements or exceeding-requirements for each of the requirements in Sections 4, 5 and 6 with the addition of a requirement to report the number and type of data breaches/data losses and the number of consumers affected. To ensure a consistent evaluation across states and to ensure the accountability of regulators to consumers, the assessment should be performed by an independent panel of cybersecurity experts.

Bias Against Consumers

In our comments on version 3 and in my colleague Peter Kochenburger's comments on version 4 of the model, we have identified a number of items in which regulators acquiesced to industry demands, creating a model biased towards Licensee interests over consumer interests. We discuss one more example here.

The definition of Cybersecurity Event excludes what we will call a "Non-Event" – a data loss by the Licensee for which the Licensee has determined that the Nonpublic Information released to an unauthorized person has not be used and has been returned or destroyed with further release. The new draft conspicuously omits the modifier "with a very high degree of certainty" for the Licensee's determination because industry opposed such a "vague" standard. Yet, the same vague standard remains with the definition of Encrypted – a low probability of assigning meaning with the key – because this vague standard was agreeable to industry.

Further, the requirement that all Cybersecurity Events be reported to the Commissioner – including those determined to by the Licensee to be "Non-Events" has been changed to eliminate reporting of the "Non-Events." The model also eliminates any requirement for the Licensee to document or justify its determination that the Cybersecurity Event was a "Non-Event." What was a limited exclusion for data breach notification when the Licensee could demonstrate with a high degree of certainty that the data loss did not result in consumer harm, has been transformed into a major loophole with no Licensee accountability to consumers or regulators.

AHIP/Blue Cross Comments

May 8, 2017

Elizabeth Kelleher Dwyer, Superintendent
Chair, NAIC Cybersecurity (EX) Drafting Group
State of Rhode Island
Department of Business Regulation
Division of Insurance
1511 Pontiac Avenue, Building 69-2
Cranston, Rhode Island 02920

Attn: Sara Robben
Via E-mail: srobben@naic.org

Re: **Insurance Data Security Model Law – Proposed Version 4**

Dear Superintendent Dwyer;

On behalf of America's Health Insurance Plans and the Blue Cross Blue Shield Association, we appreciate the opportunity to offer comments to Proposed Version 4 of the Draft NAIC Proposed Insurance Data Security Model Law.

We acknowledge and appreciate the work and progress reflected in Version 4 of the proposal. This version reflects a more sharpened focus on cybersecurity, the protection by licensees of important electronic data, and notice to regulators in the event of a breach in security. As such, this effort is now poised to make progress toward a model which can be supported by regulators, consumers, and industry. However, several problems still exist, some of which are fundamental issues existing in previous drafts which have inexplicably been carried forward into Version 4. However, all of our concerns are easily corrected without significant change to the form or purpose of the proposal.

The Need for Uniformity and Consistency. Industry has stated repeatedly that uniformity and consistency from state to state was a prerequisite to our support. Multiple provisions in Version 4 fail to meet that standard. In Section 2.A, the word "exclusive" has been deleted, so that other state standards could apply, leading not only to conflicting requirements within a state, but also between states. The language in Section 2.B and the corresponding drafting note only adds to

that confusion. We would suggest that the language in Sections 2.A and 2.B be replaced with the following:

> *The purpose and intent of this Act is to establish the exclusive state standards for data security, the investigation of a Cybersecurity Event as defined in Section 3, and notification to the Commissioner. Other applicable state laws in conflict with these requirements are hereby repealed.*

Section 11, providing that each commissioner may issue rules and regulations as necessary, also invites inconsistency from state to state. This problem has been noted before, but so has the solution: If it is apparent that a regulation will be needed to adequately implement the Model, then we should work together now to develop a companion Model Regulation to be promulgated by states along with this model proposal. In the alternative, if there are provisions in Version 4 which can readily be seen to need clarification in ways which could be done by regulation, perhaps those provisions should be clarified in the proposed Act itself.

Definitions. The definition of "Cybersecurity Event" in Section 3.C would result in notification to commissioners of every single attempt made to breach a licensee's cybersecurity system. In some companies, these may number in the thousands per day. This would be an unwarranted waste of cost and effort by both regulators and licensees. This can be resolved by deleting the words "successful or unsuccessful" in the first paragraph, and revising the third paragraph to read as follows:

Cybersecurity Event does not include an event with regard to which the Licensee has determined that the Nonpublic Information <u>has not been released to an unauthorized person, or in which any information which has been released</u> to an unauthorized person has not been used and has been returned or destroyed without further release.

The definition of "Nonpublic Information" in Section 3.I can be improved. First, the language in Section 3.I(1) is new and broader than the scope of this model, as it focuses on "Business related information of a licensee the tampering of which…would cause a material adverse impact to the business, operations or security of the licensee;…" Prior drafts of this model focused exclusively on nonpublic personal information pertaining to consumers. Unless there has been a total shift in the purpose and intent of this model, a provision focusing on the business information of a licensee, which provides no greater security or benefit to consumers, is inappropriate and misplaced, here, and should be deleted.

Additionally, the language which focuses on health information in Section 3.I(3) is overbroad. We'd suggest correcting this by revising the language as follows:

Any information or data, except age or gender, <u>which can be used to identify a particular individual</u>, in any form or medium created by or derived from a health care provider or an individual and that relates to:

…

Also, Section 3.I(3)(c) should be refined, and a new subparagraph (4), should be added, so the material reads as follows:

(c) Payment for the provision of health care to any individual *that identifies the individual; or to which there is a reasonable basis to believe the information can be used to identify the individual.*

(4) Nonpublic information does not include information that does not identify an individual, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

Lastly, the words "Risk Assessment" are used throughout this proposal, and they are capitalized as if it was a defined term. If it is to be a defined term, a definition is needed.

Information Security Program. Section 4 of Proposed Version 4 is the crux of the draft, and we have only a few corrections to suggest. First, in Section 4.D(1)(b), we'd suggest avoiding the use of a requirement for "best practices" and modify the language as follows:

Determine appropriate security measures listed in Section 4.D(2). Licensees shall use reasonable and appropriate methods for cybersecurity protection, detection, and remediation commensurate with its natures, scope, scale, and complexity.

There are also concerns with Section 4.D(2)(b). We are concerned with the use of the word, *ensure*, as it is prescriptive and implies that an entity will guaranty or warrant that these conditions are met. We have the same concern with the language in Sections 4.D(2)(e), (f), and (i). More importantly, the language in Section 4.D(2)(b) is redundant to the language in Section 4.D(3). Therefore, it should be deleted.

In addition, Section 4.D(2)(g) causes us concern. Again, prior drafts of this model focused on "multifactor authentication procedures, segregation of duties, and employee background checks for *employees*" with access to nonpublic personal information. The change to this provisions in this draft – changing "employee" to "any individual" – vastly broadens the scope of this draft without any explanation as to why. In fact, the terms "segregation of duties" and "employee background checks" make no sense when discussing "any individual". We would suggest deleting this provision and inserting the similar provision from the previous draft, which focusses on security around employees with access to this information.

Notification of Cybersecurity Event. We have a few concerns in Section 6.

First, Section 6.A would require notice to the commissioner within 72 hours of a cybersecurity event. Most states appear to have no specific time frame in their various breach statutes, but usually refer to notification to either the affected consumers or a government agency (the attorney general, the commissioner, etc.), or both, "in the most expeditious time possible and without unreasonable delay." An effective and reasonable solutions would be a requirement to notify the commissioner "in the most expeditious time possible and without unreasonable delay," combined with the HIPAA standard of "no later than 60 days." In any breach situation meeting

the definition, the first few questions asked by a regulator would likely include when was the breach discovered, and why was the commissioner not notified sooner. As all breaches are different, this language allows the commissioner to expect prompt notification without prescriptively short time limits.

Second, we propose the number of impacted residents in Section 6.A(2) should be changed to *500*.

Third, the *or* following subsection (1) should be changed to *and.*

Finally, subsection (2)(b) shares the same problem as Section 3.I(1) discussed previously, in that it appears to focus less on consumer protection, and more on the impact of the breach on the licensee. Unless, as we mentioned, the focus of this proposal has shifted away from consumer protection, we would propose that subsection (2)(b) be deleted.

Therefore, Section 6.A would read:

Notification to the Commissioner

Each Licensee shall notify the Commissioner <u>in the most expeditious time possible and without unreasonable delay, but no later than 60 days</u>, from a determination that a Cybersecurity Event has occurred if:

(1) The Licensee is an insurer domiciled in this state; <u>and</u>

(2) The Licensee reasonably believes that the Nonpublic Information involved is of <u>500</u> or more residents of this state and is a Cybersecurity Event impacting the Licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body.

In Section 6.B, we'd also recommend that, instead of the list of issues to be addressed in the notice to the commissioner, this list be deleted and Section 4 be amended to include a requirement that all licensees establish and maintain a written incident response plan as part of their Information Security Program, similar to the provisions in the New York Department of Financial Services Cybersecurity Regulation, 23 NYCRR 500.16.

Next, we strongly object to the requirement for notice to producers of record, as outlined in Section 6.F. Issues of this sort are currently matters of contract between insurers and producers, and they should remain so. Requiring this additional administrative burden on a licensee in the midst of responding to a cybersecurity event is unrealistic and unnecessary.

Confidentiality. As stated previously, we support the modifications made to Section 8 in order to specify which materials involved in a data breach would be confidential, and acknowledge that these changes clarify that some of the information coming into a commissioner's possession may not necessarily be confidential. However, other areas in the confidentiality provisions of Version 4 are substantive variances from the so-called "ORSA protections." We continue to maintain that highly confidential materials related to an entity's information security program and possible breach are just as deserving of strong protections as the highly confidential ORSA-related materials submitted to a commissioner. Additionally, since some information involved in a data breach may be shared with other state regulators, it is vital that NAIC models utilizing confidentiality protection provisions maintain consistency not only between those models, but also from state to state in each state's enactment of the model law. Variations and complete omissions include a missing closing sentence in Section 8.A ("*The commissioner shall not otherwise make the documents, materials, or other information public without the prior written*

consent of the insurer."), the use of "may" instead of "shall" in Section 8.C(3), and the omission of the entire ORSA Model Sections 8.C(3)(i) - (vi), 8.D, and 8.F. To assist in your review, we have included **Section 8. Confidentiality**, of the ORSA Model, as an Appendix, highlighting the portions which vary, or were omitted entirely, from Proposed Version 4.

We thank you for your time and consideration of our views, and we look forward to continuing our work with you on the development of the Model.

Sincerely,

Bob Ridgeway
America's Health Insurance Plans

Paul S. Brown
Blue Cross Blue Shield Association

Appendix
ORSA Section 8. Confidentiality

Section 8. Confidentiality.

A. Documents, materials or other information, including the ORSA Summary Report, in the possession of or control of the Department of Insurance that are obtained by, created by or disclosed to the commissioner or any other person under this Act, is recognized by this state as being proprietary and to contain trade secrets. All such documents, materials or other information shall be confidential by law and privileged, shall not be subject to [insert open records, freedom of information, sunshine or other appropriate phrase], 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 official duties. The commissioner shall not otherwise make the documents, materials or other information public without the prior written consent of the insurer.

B. Neither the commissioner nor any person who received documents, materials or other ORSA-related information, through examination or otherwise, while acting under the authority of the commissioner or with whom such documents, materials or other information are shared pursuant to this Act shall be permitted or required to testify in any private civil

action concerning any confidential documents, materials, or information subject to subsection A.

C. In order to assist in the performance of the commissioner's regulatory duties, the commissioner:

(1) May, upon request, share documents, materials or other ORSA-related information, including the confidential and privileged documents, materials or information subject to subsection A, including proprietary and trade secret documents and materials with other state, federal and international financial regulatory agencies, including members of any supervisory college as defined in the [insert cross-reference to appropriate section of Insurance Holding Company System Regulatory Act, as amended], with the NAIC and with any third-party consultants designated by the commissioner, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the ORSA-related documents, materials or other information and has verified in writing the legal authority to maintain confidentiality; and

(2) May receive documents, materials or other ORSA-related information, including otherwise confidential and privileged documents, materials or information, including proprietary and trade-secret information or documents, from regulatory officials of other foreign or domestic jurisdictions, including members of any supervisory college as defined in the [insert cross- reference to appropriate section of Insurance Holding Company System Regulatory Act, as amended], and from the NAIC, and shall maintain as confidential or privileged any documents, 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 document, material or information.

(3) Shall enter into a written agreement with the NAIC or a third-party consultant governing sharing and use of information provided pursuant to this Act, consistent with this subsection that shall:

(i) Specify procedures and protocols regarding the confidentiality and security of information shared with the NAIC or a third-party consultant pursuant to this Act, including procedures and protocols for sharing by the NAIC with other state regulators from states in which the insurance group has domiciled insurers. The agreement shall provide that the recipient agrees in writing to maintain the confidentiality and privileged status of the ORSA-related documents, materials or other information and has verified in writing the legal authority to maintain confidentiality;

(ii) Specify that ownership of information shared with the NAIC or a third-party consultant pursuant to this Act remains with the commissioner and the NAIC's or a third-party consultant's use of the information is subject to the direction of the commissioner;

(iii) Prohibit the NAIC or third-party consultant from storing the information shared pursuant to this Act in a permanent database after the underlying analysis is completed;

(iv) Require prompt notice to be given to an insurer whose confidential information in the possession of the NAIC or a third-party consultant pursuant to this Act is subject to a request or subpoena to the NAIC or a third-party consultant for disclosure or production;

(v) Require the NAIC or a third-party consultant to consent to intervention by an insurer in any judicial or administrative action in which the NAIC or a third-party consultant may be required to disclose confidential information about the insurer shared with the NAIC or a third-party consultant pursuant to this Act; and

(vi) In the case of an agreement involving a third-party consultant, provide for the insurer's written consent.

D. The sharing of information and documents by the commissioner pursuant to this Act shall not constitute a delegation of regulatory authority or rulemaking, and the commissioner is solely responsible for the administration, execution and enforcement of the provisions of this Act.

E. No waiver of any applicable privilege or claim of confidentiality in the documents, proprietary and trade-secret materials or other ORSA-related information shall occur as a result of disclosure of such ORSA-related information or documents to the commissioner under this section or as a result of sharing as authorized in this Act.

F. Documents, materials or other information in the possession or control of the NAIC or a third-party consultants pursuant to this Act shall be confidential by law and privileged, shall not be subject to [insert open records, freedom of information, sunshine or other appropriate phrase], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action.

IRI Comments

Insured Retirement Institute
1100 Vermont Avenue, NW | 10th Floor
Washington, DC 20005
t | 202.469.3000
f | 202.469.3030

May 8, 2017

Sara Robben
NAIC Central Office
1100 Walnut Street
Kansas City, MO 64106-2197
Via email: srobben@naic.org

Re: Comments on Insurance Data Security Model Law Version 4

Dear Ms. Robben:

On behalf of our members, the Insured Retirement Institute ("IRI")[1] respectfully submits these comments regarding the fourth version of the Insurance Data Security Model Law (the "model"). IRI acknowledges and appreciates the extraordinary effort the Cybersecurity Task Force has put towards a drafting a model law. IRI and its members commend the decision to focus solely on data security provisions in this fourth version of the model law. IRI believes this version provides a path towards our shared goal of protecting consumers' personal information against data security breaches.

Although this version demonstrates progress from previous versions, we continue to believe that the model should provide exclusive standards that supersede any provision of current state law or regulation, providing uniformity from state to state. IRI anticipates submitting detailed comments pertaining to exclusivity and definitions when the draft model law is released for a formal exposure.

Thank you for the opportunity to provide these comments. Please feel free to contact me at (202) 469-3032 or ccrucitti@irionline.org if you have any questions or to discuss this matter further.

Sincerely,

Chelsea Crucitti
Vice President, State Affairs
Insured Retirement Institute (IRI)

[1] IRI is the only national trade association that represents the entire supply chain of the retirement income industry. IRI has more than 500 member companies, including major life insurance companies, broker-dealers, banks, and asset management companies. IRI member companies account for more than 95% of annuity assets in the United States, include the top 10 distributors of annuities ranked by assets under management, and are represented by more than 150,000 financial professionals serving over 22.5 million households in communities across the country.

Peter Kochenburger and CEJ Comments

Comments of Peter Kochenburger and the Center for Economic Justice
To the NAIC Cybersecurity Model Law Drafting Group
May 8, 2017

The Cybersecurity Working Group (WG) formed the ad-hoc drafting group with the understanding that a model law in this area should incorporate the perspectives and concerns of multiple stakeholders, including regulators, insurance producers, insurers, reinsurers, and consumers. In our April 17, 2017 comments to the Cybersecurity Working Group (attached) we discussed concerns with bifurcating the Data Security Model draft, and if bifurcation was to occur, the Working Group's commitment that it would proceed to draft consumer protection requirements as soon as the data security section is completed.

We reiterate our concern that the refusal to compromise by some industry members has succeeded in blocking the most fundamental protections consumers require: prompt and effective notice that their personal information has likely been stolen from their insurer or its vendors, and remedies that address the harm. We know regulators share our objectives, but they will not be achieved if Version 4 will be the final product of the drafting group.

Comments on Draft Version 4[1]

The Working Group draft now incorporates significant sections of the Cybersecurity Requirements for Financial Services Companies recently promulgated by the New York Department of Financial Services (NY Cyber Regulations), including Sections 3.H – J, Section 4.f, and Section 6.A. As we previously noted, there are advantages in utilizing the NY Cyber Regulations as a template for the NAIC model in the data security (pre-breach) area. We also support the new provision requiring Licensees to maintain records related to a Cybersecurity Event for five years (Section 5.D), though NY Cyber Regulations 500.06, Audit Trail, is more detailed and we recommend this section be incorporated in its entirety.

We also note that Draft version 4 contains the "250 or more residents" requirement as a prerequisite to notification to Commissioners in other states (Section 6.A (2). There is no similar limitation in the NY Cyber Regulations and incorporating one in the NAIC model could prevent Commissioners in other states from learning of some cyber breach affecting their residents, and investigating to determine to their satisfaction the extent and type of harm suffered by residents of their state.

In addition, Version 4 maintains the unnecessarily broad Confidentiality language that we (and several state insurance departments) have commented on before; the NY Cyber Regulations provide a more appropriate model simply by incorporating existing confidentiality provisions

[1] The need for public outcome performance measures evaluating the effectiveness of a Licensee's Data Security Program is addressed in separate comments filed by CEJ, and we will not reiterate them here.

applicable to regulated entities.[2] We all agree that the methods of a cyber breach and the personal information data stolen should not be publicly available, but the current draft language likely sweeps too far and could unnecessarily immunize important information and testimony in subsequent investigations and litigation.

The New York Cyber Regulations do not contain the detailed consumer notification provisions contained in earlier versions of the NAIC model. The reason is not because the issue is too controversial, but that New York already has a broad, mandatory consumer notification requirement applicable to insurers, and the Regulations require Licensees to incorporate consumer notification plans in their Cybersecurity Program (see Sections 500.02(b)(6), 500.03(n), and 500.16 – Incident Response Plan).[3] Accordingly, New York Cyber laws go as far as they can in requiring insurers to notify New York consumers of a Cybersecurity event.

In contrast, the new provision in Version 4 of the NAIC draft incorporating state data breach notification laws (end of Section 6.B) does not model or reflect New York law in this area, as it would leave insurance consumers nationwide with inconsistent, sometimes insufficient, and in a few states, non-existent data breach notification requirements for insurance entities. This is a very different result than developing a notification model that would combine best practices in this area, and provide a nationwide standard promoting both a high level of consumer protection and consistency. At best this version maintains the status quo – a multitude of different state requirements applicable – or not – to insurers and insurance intermediaries.[4]

---

[2] "Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law or any other applicable state or federal law." NY Cyber Regulations Section 500.18

[3] We discussed this issue more extensively in pages 4-5 of our April 17, 2017 comments.

[4] However, this provision is preferable to omitting any reference to state notification laws, as we noted in our April 17, 2017 comments (page 5).