Draft: ~~3/28~~/17/2016 (version 2)
~~Draft of New Cybersecurity~~A new model: Insurance Data Security Model Law
Cybersecurity (EX) Task Force

Comments are being requested on this draft by Friday, September 16, 2016. Comments should be sent by email to Sara Robben at srobben@naic.org.

INSURANCE DATA SECURITY MODEL LAW

Table of Contents

Section 1. Title

This act shall be known and may be cited as the "Insurance Data Security Act."

Section 2. Purpose and Intent

~~The~~Notwithstanding any other provision of law including [insert reference to state's general data security breach notification law], the purpose and intent of this Act is to establish the exclusive standards in this state for data security and investigation and notification of a data breach ~~of data security~~ applicable to licensees, as defined in ~~this state.~~

Section ~~2.~~ ~~Applicability and Scope~~

~~Consistent with authority to regulate the business of insurance pursuant to the McCarran Ferguson Act, 15 U.S.C. § 1011 et seq. and the laws of this state, this~~3G. This Act ~~is intended to regulate the business of insurance. No other provision of state~~ shall not be construed as superseding, altering, or ~~federal law or~~ affecting any statute, regulation ~~regarding data security~~, order or interpretation of law in this state, except to the extent that such statute, regulation, order or ~~investigation or notification of a breach of data security shall apply to licensees subject to the~~ interpretation is inconsistent with the provisions of this Act~~.~~ and then only to the extent of the inconsistency. A state statute, regulation, order or interpretation is not inconsistent with the provisions of this Act if the protection such statute, regulation, order or interpretation affords any person is greater than the protection provided under this Act.

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

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

~~A. "Breach of data security," "breach," "data breach," or "security breach" means the unauthorized acquisition of personal information.~~

~~The term "breach of data security" does not include the unauthorized acquisition of personal information that is encrypted, redacted, or otherwise protected by another method that renders the information unreadable and unusable if the encryption, redaction, or protection process or key is not also acquired without authorization.~~

~~B.~~A. "Consumer" means an individual ~~or entity~~, including but not limited to applicants, policyholders ~~and their family members.~~ , insureds, beneficiaries, claimants, certificate holders and others whose personal information is in a licensee's possession, custody or control.

~~C.~~B. "Consumer reporting agency" has the same meaning as "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

C. "Data breach" means the unauthorized acquisition, release or use of personal information.

The term "data breach" does not include the unauthorized acquisition, release or use of encrypted personal information if the encryption, process or key is not also acquired, released or used without authorization.

D. "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

E. "Harm or inconvenience" means any of the following or the reasonable likelihood thereof:

(1) Identity theft;

(2) Fraudulent transactions on financial accounts~~rendered unusable, unreadable, or indecipherable~~; or

(3) Other misuse as defined by [insert state definition of misuse or comparable term, if applicable].

Drafting Note: Several states have defined the term "misuse" in state law and can refer to ~~an unauthorized~~ this in Section 3E(3). If a state does not have this term defined, they may consider either deleting that paragraph or defining misuse above using a definition similar to that of other states. For example, see 17-A Me. Rev. Stat. § 905-A, which provides that

A person ~~through a security technology or methodology generally accepted in the field of information security.~~ is guilty of misuse of identification if, in order to obtain confidential information, property or services, the person intentionally or knowingly:

A. Presents or uses a credit or debit card that is stolen, forged, canceled or obtained as a result of fraud or deception;
B. Presents or uses an account, credit or billing number that that person is not authorized to use or that was obtained as a result of fraud or deception; or
C. Presents or uses a form of legal identification that that person is not authorized to use.

~~E.~~F. "Information security program" means the ~~administrative, technical, or physical~~ safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.

~~F.~~G. "Licensee" means ~~all~~any person or entity licensed ~~insurers, producers and other persons licensed~~, authorized to operate, or registered, or required to be licensed, ~~or authorized or required to be~~ authorized, or registered ~~or required to be registered~~ pursuant to the ~~Insurance Law~~insurance laws of this state.

~~G.~~H. "Personal Information" means:

(1) A financial account number relating to a consumer, including a credit card number or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account; or

(2) Information including:

The first name or first initial and last name of a consumer in combination with:

(a) The consumer's non-truncated social security number;

(b) The consumer's driver's license number, passport number, military identification number, or other similar number ~~issued~~ on a government-issued document ~~used to verify identity~~;

(c) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online or financial account of the consumer;

(d) Biometric data of the consumer ~~used to gain~~that would permit access to financial accounts of the consumer;

(e) ~~Health~~Any information of the consumer that the licensee has a legal or contractual duty to protect from unauthorized access or public disclosure;

~~(e)~~(f) The consumer's date of birth;

~~(f)~~(g) Information that the consumer provides to a licensee to obtain an insurance product or service used primarily for personal, family, or household purposes from the licensee;

~~(g)~~(h) Information about the consumer resulting from a transaction involving an insurance product or service used primarily for personal, family, or household purposes between a licensee and the consumer;

~~(h)~~(i) Information the licensee obtains about the consumer in connection with providing an insurance product or service used primarily for personal, family, or household purposes to the consumer; or

~~(i)~~(j) A list, description, or other grouping of consumers (and publicly available information pertaining to them), that is derived using the information described in ~~[Subparagraphs (f~~Section 3H(2)(g) through (~~h), information provided to licensees]~~i), that is not publicly available.

(3) Any of the data elements identified in Section 3H(2)(a) through (f) when not in connection with the consumer's first name or initial and last name, if those elements would be sufficient to permit the fraudulent assumption of the consumer's identity or unauthorized access to an account of the consumer.

~~(3)~~(4) Any information or data except age or gender, that relates to:

(a) The past, present or future physical, mental or behavioral health or condition of a consumer;

(b) The provision of health care to a consumer; or

(c) Payment for the provision of health care to a consumer.

The term "personal information" does not include publicly available information that is lawfully made available to the general public and obtained from federal, state, or local government records; or widely distributed media.

~~H. "Substantial harm or inconvenience" means~~

~~(1) Identity theft; or~~

~~(2) Fraudulent transactions on financial accounts.~~

I. "Third-party service provider" ~~or "service provider"~~ means a person or entity that ~~maintains, processes~~contracts with a licensee to maintain, process, store or otherwise ~~is permitted~~have access to personal information ~~through its provision of services directly to~~under the ~~licensee~~licensee's possession, custody or control.

Section 4. Information Security Program

A. Implementation of an Information Security Program

~~Each~~Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities and the sensitivity of the personal information in the licensee's possession, custody or control, each licensee shall develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for the protection of personal information. ~~-~~The licensee shall document, on an ongoing basis, compliance with its information security program.

B. Objectives of Information Security Program

A licensee's information security program shall be designed to:

(1) ~~Ensure~~Protect the security and confidentiality of personal information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information; ~~and~~

(3) Protect against unauthorized access to or use of ~~the~~personal information ~~that could result in substantial~~, and minimize the likelihood of harm or inconvenience to any ~~customer.~~consumer; and

~~C. Appropriateness of Information Security Program~~

~~The scale~~Define and ~~scope of~~periodically reevaluate a ~~licensee's~~schedule for retention of personal information ~~security program shall be appropriate to:~~

~~(1)~~(4) ~~The size~~ and ~~complexity of the licensee;~~a mechanism for its destruction when no longer needed.

~~(2) The nature and scope of the activities of the licensee; and~~

~~(3) The sensitivity of the consumer information to be protected.~~

~~D.~~C. Risk Assessment

The licensee shall:

(1) Designate an employee or employees ~~to coordinate~~responsible for the information security program;

(2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of personal information or personal information systems;

(3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

(4) Assess the sufficiency of policies, procedures, personal information systems and other safeguards in place to ~~control~~manage these ~~risks~~threats, including consideration of ~~risks~~threats in each relevant area of the licensee's operations, including:

(a) Employee training and management;

(b) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and

(c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(5) ~~Design and implement~~Implement information safeguards to ~~control~~manage the ~~risks~~threats identified in its ~~risk~~ assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures.

~~E.~~D. Risk Management

The licensee shall, at a minimum:

(1) Design its information security program to ~~control~~mitigate the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities, ~~using as a guide, the *Framework for Improving Critical Infrastructure Cybersecurity* developed by the National Institute of Standards and Technology (NIST),~~based on generally accepted cybersecurity principles, including ~~adopting~~ the following security measures, as appropriate:

(a) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent ~~employees from providing~~the unauthorized acquisition, release or use of personal information to or by employees or unauthorized individuals ~~who may seek to obtain this information through fraudulent means~~outside of the licensee;

(b) Restrict access at physical locations containing personal information, ~~such as buildings, computer facilities, and records storage facilities, to permit access~~ only to authorized individuals;

(c) Encrypt ~~electronic~~all personal information~~, including~~ while ~~in transit~~being transmitted on a public internet network or ~~in storage on networks~~ wirelessly and all personal information stored on a laptop computer or ~~systems to which unauthorized individuals may have access~~other portable computing or storage device or media;

(d) ~~Design procedures to ensure~~Ensure that information system modifications are consistent with the licensee's information security program;

(e) Utilize state of the art techniques, such as multi-factor authentication procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, personal information;

(f) Regularly test or monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(g) Implement response ~~programs~~procedures that specify actions to be taken when the licensee suspects or detects that unauthorized individuals have gained access to information systems;

(h) Implement measures to protect against destruction, loss, or damage of personal information due to ~~potential~~ environmental hazards, such as fire and water damage or technological failures; and

(i) Develop, implement, and maintain ~~appropriate measures to properly dispose~~procedures for the secure disposal of personal information~~;~~ in any format.

(2) ~~Address~~Include cybersecurity risks ~~into~~in the licensee's enterprise risk management process; and

(3) ~~Use an Information Sharing and Analysis Organization (ISAO)~~Use generally accepted cybersecurity principles to share information and stay informed regarding emerging threats or vulnerabilities.

~~F.~~E. Oversight by Board of Directors

If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

~~(a) Approve the licensee's written information security program; and~~

(1) ~~(b)~~ Oversee the development, implementation, and maintenance of the licensee's information security program, including assigning specific responsibility for ~~its implementation and reviewing reports from~~the plan to the licensee's executive management~~.~~; and

(2) ~~If~~Require the ~~licensee has a board of directors, the licensee shall~~ licensee's executive management to report ~~to its board or an appropriate committee of the board~~in writing at least annually, the following information:

(a) ~~(a)~~ The overall status of the information security program and the licensee's compliance with this Act; and

~~(c)~~(b) Material matters related to ~~its~~ the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, ~~security~~data breaches or violations and management's responses thereto, and recommendations for changes in the information security program.

~~G.~~F. Oversight of Third-Party Service Provider Arrangements

The licensee shall~~:~~

~~(1) Select and retain~~ contract only with third-party service providers that are capable of maintaining appropriate safeguards for ~~the~~ personal information ~~at issue;~~

~~(2) Require~~ in the licensee's possession, custody or control, and the licensee shall be responsible for any failure by such third-party service providers to ~~do the following, by contract:~~

~~(a) Implement and maintain appropriate safeguards for the~~protect personal information ~~at issue, including those security measures listed in [Section 4E(1), Risk Management].~~

~~(b) Notify licensee within three (3) calendar days of a discovery of a breach of data security in a system maintained~~provided by the licensee to the third-party service ~~provider that has been contracted to maintain, store, or process data containing personal information on behalf of a licensee;~~

~~(c) Indemnify licensee in the event of a cybersecurity incident that results in loss;~~

~~(d) Allow licensee or its agents to perform cybersecurity audits of the third party service provider; and~~

~~(c) Represent and warrant its compliance with all requirements; and~~

~~Oversee or obtain an assessment of the third-party service provider's compliance~~providers consistent with ~~contractual obligations, where appropriate in light of the licensee's risk assessment~~this Act.

~~H.~~G. Program Adjustments

The licensee shall monitor, evaluate and adjust, as appropriate, the information security program ~~in light of~~consistent with any relevant changes in technology, the sensitivity of its personal information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to personal information systems.

Section 5. ~~Consumer Rights Before~~ Investigation of a Data Breach ~~of Data Security~~

~~A. The licensee shall provide consumers with information regarding~~ If the ~~types of personal information collected and stored by licensee or any third party service providers it contracts with.~~

~~B. The licensee shall post its privacy policy on its websites and make it available to consumers in hard copy, upon request. The privacy policy shall explain what type of personal information licensee collects, what options consumers have about their data, how consumers can review and change or correct their data if needed, how the data is stored and protected, and what consumers can do if the licensee does not follow its privacy policy.~~

licensee learns~~**Section 6. Investigation of a Breach of Data Security**~~

A. ~~If a licensee believes~~ that a data breach ~~of data security~~ has or may have occurred in relation to personal information ~~that is maintained, communicated,~~in the possession, custody or ~~otherwise handled by, or on behalf~~control of~~,~~ the licensee or any of the licensee's third-party service providers, the licensee shall conduct ~~an~~a prompt investigation.

B. During the investigation, the licensee shall, at a minimum:

(1) Assess the nature and scope of the ~~incident~~data breach or potential data breach;

(2) Identify any personal information that may have been involved in the ~~incident~~data breach;

(3) Determine ~~if~~whether the personal information has been acquired, released or used without authorization; and

(4) ~~Take~~Perform or oversee reasonable measures to restore the security ~~and confidentiality~~ of the information systems compromised in the data breach in order to prevent further unauthorized acquisition, release or use of personal information in the licensee's possession, custody or control.

Section 6. Notification of a Data Breach

If following an investigation under Section ~~**7. Notification of a Breach of Data Security**~~

A. ~~If~~5, the licensee determines ~~under [~~that an unauthorized acquisition of personal information listed in Section ~~6, Investigation of~~ 3H(1), (2)(a ~~Breach of Data Security] that the unauthorized acquisition of personal information~~) through (f), (3) or (4) involved in a ~~breach of data security is reasonably likely to cause substantial harm or inconvenience to the consumers to whom the information relates~~data breach has occurred, the licensee, or a third party acting on behalf of the licensee, shall notify~~, without unreasonable delay~~:

(1) ~~An appropriate~~ All consumers to whom the personal information relates;

(2) The insurance commissioner in the licensee's state of domicile and the insurance commissioners of all the states in which a consumer whose information was or may have been compromised resides;

~~(1)~~(3) The relevant Federal and state law enforcement ~~agency~~agencies, as appropriate;

~~(2) The insurance commissioner;~~

~~(3)~~(4) Any relevant payment card network, if the data breach involves ~~a breach of~~ payment card numbers; and

~~(4)~~(5) Each consumer reporting agency ~~that compiles and maintains files on consumers on a nationwide basis, if the~~, if the data breach involves personal information relating to ~~1,000~~500 or more consumers~~; and~~.

~~(5) All consumers to whom the personal information relates.~~

B. ~~Providing Notice~~Notification to the Commissioner

~~No~~Notwithstanding the responsibilities prescribed in Sections 5A and 6A of this Act, no later than ~~five (5) calendar~~three (3) business days ~~of identifying~~after determining that a data breach has occurred, the licensee shall notify the commissioner~~, providing as~~ that a data breach has occurred. The licensee shall provide as much of the following information as ~~is known to the licensee~~possible:

(1) Date of the data breach;

(2) Description of the data breach, including how the information was exposed, whether lost, stolen, or breached;

(3) How the data breach was discovered;

(4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(5) The identity of the source of the data breach;

~~(5)~~ Whether ~~any individuals involved in the incident (both internal and external) have been identified;~~

(6) ~~Whether~~licensee has filed a police report ~~has been filed~~or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(7) Description of the type of information lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc.);

~~(8)~~ Whether, if the information was encrypted~~;~~

(8) ~~The time period covered by~~, the encryption, redaction or protection process or key was also acquired without authorization;

(9) The period during which the information ~~that was lost, stolen or breached~~system was compromised by the data breach;

(10) ~~Number~~The number of ~~residents~~total consumers and consumers of ~~the~~each state affected by the data breach;

(11) ~~Results~~The results of any internal review identifying ~~either~~ a lapse in either automated controls or internal procedures, or ~~confirmation~~confirming that all automated controls or internal procedures were followed;

(12) Identification of ~~remedial~~ efforts being undertaken to ~~cure~~remediate the situation which permitted the ~~information security incident~~data breach to occur;

(13) ~~Copies~~A copy of the licensee's privacy ~~policies and data breach~~ policy~~;~~ and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the data breach; and

(14) Name of a contact person who is both familiar with the ~~details~~data breach and ~~able~~authorized to ~~authorize actions~~act for the licensee~~; and~~.

~~(15) Other regulatory or law enforcement agencies that have been notified and when notification was provided.~~

~~Providing Notice~~The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning the data breach.

C. Notification to Consumer Reporting Agencies

~~No later than sixty (60) calendar days of identifying a data breach, the~~The licensee shall notify, as expediently as possible and without unreasonable delay, after determining that a data breach has occurred, each consumer reporting agency ~~that compiles and maintains files on consumers on a nationwide basis, if the~~ , if the data breach involves personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) relating to ~~[1000]~~500 or more consumers. Notification must include the date of the data breach, an estimate of the number of persons affected by the data breach, if known, and the actual or anticipated date that persons were or will be notified of the data breach.

D. ~~Providing Notice~~Notification to Consumers

(1) ~~No~~The licensee shall notify all consumers whose personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) was affected as expediently as possible and without unreasonable delay, and in no case later than sixty (60) calendar days ~~of identifying~~after determining that a data breach~~, the licensee shall notify all affected consumers.~~ has occurred.

~~(2) Licensee will provide~~Prior to sending the notification ~~in writing by first class mail, unless the consumer has agreed to be contacted through e-mail.~~

~~(3)~~(2) ~~No later than forty five (45) calendar days of identifying a data breach~~, the licensee shall provide ~~to~~ the commissioner~~,~~ with a draft of the proposed written communication to consumers. The commissioner shall have the right to ~~edit~~review the proposed communication before the licensee sends it to consumers~~. This proposed notification shall be written in plain English~~, to ensure compliance with this subsection and ~~include~~to prescribe the ~~following information:~~appropriate level of consumer protection pursuant to Section 7.

The notice must be written in straightforward language and include the following information::

(a) A description of the type of information involved in the data breach;

(b) A description of the action that the licensee or ~~business it contracts with~~third-party service provider has taken to safeguard the information;

(c) A summary of rights of victims of identity theft prepared under § 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g(d));

(d) The steps consumers can take to protect themselves from identity theft or fraud, which shall include an explanation that consumers shall have a right to do the following:

(i) ~~Put~~Place a 90-day initial fraud alert on their ~~credit~~consumer reports;

(ii) ~~Put~~Place a seven-year extended fraud alert on their ~~credit~~consumer reports;

(iii) ~~Put~~Place a credit freeze on their ~~credit report~~consumer reports;

(iv) ~~Get~~Have a free copy of their ~~credit~~consumer report from each credit bureau;

(v) ~~Get~~Receive fraudulent information related to the data breach removed (or "blocked") from their ~~credit~~consumer reports;

(vi) Dispute fraudulent or wrong information on their ~~credit~~consumer reports;

(vii) Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach;

(viii) ~~Get~~Receive copies of documents related to the identity theft; and

(ix) Stop ~~a debt collector~~contacts from ~~contacting them~~debt collectors related to the data breach;

(e) Contact information for the three nationwide consumer reporting agencies;

(f) Contact information for the licensee or its designated call center; and

(g) An offer from the licensee to the consumer to provide appropriate identity theft protection services free of cost to the consumer for a period of not less than twelve (12) months, if appropriate, or other consumer protections ordered by the commissioner pursuant to Section 7 of this Act.

(3) ~~Providing~~ The licensee will provide the consumer notification:

(a) In writing by first class mail; or

(b) Electronically if the consumer has agreed to be contacted through e-mail or other means pursuant to [insert reference to state Electronic Transactions Act.]; or

(c) By substitute method, if the licensee demonstrates to the commissioner's satisfaction that the cost of providing notice by Section 6D(3)(a) or (b) would be excessive or that another legitimate reason exists for substitute notice. The substitute method must include conspicuous posting of the notice on the licensee's publicly accessible website and publication in statewide media in this state.

E. Notice Regarding Data Breaches of Third-Party Service Providers

~~Licensee shall comply with [Subsections B and D] by notifying the commissioner and consumers in~~ In the event of a data breach ~~of data security~~ in a system maintained by a third-party service provider~~.~~, the licensee shall comply with Section 6A through D. The computation of licensee's deadlines shall begin on the day after the third-party service provider ~~provides notice to licensee~~notifies the licensee of the data breach or the licensee otherwise has actual knowledge of the data breach, whichever is sooner.

F. Notwithstanding the requirements of ~~[Subsections C~~Section 6C, D, and E~~],~~ notice may be delayed where requested by an appropriate state or federal law enforcement agency. The commissioner shall be notified of any such request.

Drafting Note: Section ~~8~~5 and Section 6 may be duplicative of current state law. Each state should conduct its own analysis to determine whether or not Section 5 and Section 6, in whole or in part, are necessary to be included in its statutes.

Section 7. Consumer Protections Following a Data Breach ~~of Data Security~~

After reviewing the licensee's data breach notification, the commissioner shall prescribe the appropriate level of consumer protection required following the data breach and ~~for what period of time~~how long that protection will be provided. ~~At a minimum,~~The commissioner may order the licensee ~~will~~to offer to pay for ~~at least~~ twelve (12) months or more of identity theft protection for affected consumers, pay for a credit freeze, or take other action deemed necessary to protect consumers.

Drafting Note: Many states have statutes providing that a consumer reporting agency cannot charge a fee for a credit freeze on a consumer file when the consumer is a victim of identity theft, which is shown by providing a police report. For an example, *see* Tex. Bus. & Com. Code § 20.04(b). As an alternative to having the licensee pay for the credit freeze, a state should consider referencing that law and providing that the credit freeze is free for consumers after the data breach is reported to law enforcement by the licensee, by showing a data breach notification letter from the licensee. The state may also need to amend its free credit freeze law to ensure this is covered.

If the data breach has affected consumers in other states, the commissioner shall, consistent with the requirements of [reference to statute describing the commissioner's general powers] and with the circumstances of the data breach as they affect consumers in this state, cooperate with the insurance regulators of those states in prescribing the appropriate level of consumer protection described in the previous sentence.

Section ~~9~~8. Power of Commissioner

The commissioner shall have power to examine and investigate into 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].

~~**Section 10. Hearings, Witnesses, Appearances, Production of Books and Service of Process**~~

~~A.~~ **Section 9. Enforcement**

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 ~~shall~~may issue and serve upon such licensee 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.~~The hearing shall be conducted in accordance with [cite provisions of state administrative procedure act or insurance code applicable to administrative enforcement proceedings for serious violations].

~~B. At the time and place fixed for such hearing the licensee 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.~~

~~C. 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 which are relevant to the hearing. A stenographic record of the hearing shall be made upon the request of any party or at the discretion of the commissioner. If no stenographic 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.~~

~~D. 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 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 postcard receipt in the case of registered mail, shall be sufficient proof of service.~~

Section ~~11~~10. Confidentiality

A. Any documents, materials or other information in the control or possession of the department of insurance that ~~is~~are furnished by a licensee or an employee or agent thereof acting on behalf of licensee~~, or~~ pursuant to Section 6B(2), (3), (4), (5), (6), (8), (11), and (12), or that are obtained by the insurance commissioner in an investigation or examination pursuant to Section 8 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 ~~phrase~~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 insurance 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 insurance commissioner's duties.

B. Neither the insurance commissioner nor any person who received documents, materials or other information while acting under the authority of the insurance commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to ~~[Subsection A].~~Section 10A.

C. In order to assist in the performance of the insurance commissioner's duties under this Act, the insurance commissioner:

(1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to ~~[Subsection A],~~Section 10A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees to maintain the confidentiality and privileged status of the document, material or other information;

(2) May receive documents, materials or information, including otherwise confidential and privileged documents, 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 document, material 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; and

(3) **[OPTIONAL]** May enter into agreements governing sharing and use of information consistent with this subsection.

D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in ~~[Subsection C].~~Section 10C.

E. Nothing in this Act shall prohibit the insurance commissioner from releasing final, adjudicated actions including for cause terminations 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~~ of the National Association of Insurance Commissioners~~.

~~**Section 12. Cease and Desist Orders and Reports**~~

~~A. If, after a hearing pursuant to Section [section on hearings], the commissioner determines that the licensee 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 a copy of such findings and an order requiring such licensee to cease and desist from the conduct or practices constituting a violation of this Act.~~

~~B. If, after a hearing pursuant to Section [section on hearings], the commissioner determines that the licensee 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~~

licensee 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 under Section [section on judicial review] of this Act for filing a petition for review or until such petition is actually 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 under Section [section on judicial review] of this Act 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.

Section 13. Penalties

A. In any case where a hearing pursuant to Section [section on hearings] results in the finding of a knowing violation of this Act, the commissioner may, in addition to the issuance of a cease and desist order as prescribed in Section [section on cease and desist orders], order payment of a monetary penalty of not more than [$500] for each violation but not to exceed [$10,000] in the aggregate for multiple violations.

B. Any person who violates a cease and desist order of the commissioner under Section [section on cease and desist orders] of this Act may, after notice and hearing and upon order of the commissioner, be subject to one or more of the following penalties, at the discretion of the commissioner:

(1) A monetary fine of not more than [$10,000] for each violation;

(2) A monetary fine of not more than [$50,000] if the commissioner finds that violations have occurred with such frequency as to constitute a general business practice; or

(3) Suspension or revocation of an insurance institution's or agent's license.

C. Notwithstanding the foregoing, nothing in this Act shall be construed to limit the commissioner's authority under [insert citation to Unfair Trade Practices Act].

Section 14. Judicial Review of Orders and Reports

A. Any licensee subject to an order of the commissioner under Section [section on cease and desist orders] or Section [section on penalties] or any licensee 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 forthwith certify and file in such court a transcript of 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 transcript 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 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 under Section [section on cease and desist orders] or [section on penalties] 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 to the extent provided in Section [section on cease and desist orders]; 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 licensee affected by such order or report from any liability under any law of this state.~~

~~**Section 15. Individual Remedies**~~

~~A. If any licensee fails to comply with Section [insert section(s) addressing consumer rights] of this Act with respect to the rights granted under those sections, any person whose rights are violated may apply to the [insert title] Court of this state, or any other court of competent jurisdiction, for appropriate equitable relief.~~

~~B. In any action brought pursuant to this section, the court may award the cost of the action and reasonable attorney's fees to the prevailing party.~~

~~C. An action under this section must be brought within two (2) years from the date the alleged violation is or should have been discovered.~~

~~D. Except as specifically provided in this Act, there shall be no remedy or recovery available to consumers, in law or in equity, for occurrences constituting a violation of any provisions of this Act.~~

~~**Section 16. 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 a licensee; provided, however, this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person.~~

~~**Section 17. Obtaining Information Under False Pretenses**~~

~~Any person who knowingly and willfully obtains information about a consumer from a licensee under false pretenses shall be fined not more than [$10,000] or imprisoned for not more than one year, or both.~~

~~**Section 18**~~Drafting Note: States conducting an investigation or examination under their examination law may apply the confidentiality protections of that law to such an investigation or examination.

Section 11. Penalties

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

Section 12. Rules and Regulations

The commissioner may, upon notice and opportunity for all interested persons to be heard, issue such rules, regulations and orders as shall be necessary to carry out the provisions of this Act.

Section ~~19~~13. Severability

If any provisions of this Act or the application thereof 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 thereby.

Section ~~20~~14. Effective Date

This Act shall take effect on [insert a date which allows at least a one year interval between the date of enactment and the effective date].