Senate

General Assembly

File No. 320

January Session, 2019

Senate Bill No. 903

Senate, April 2, 2019

The Committee on Insurance and Real Estate reported through SEN. LESSER of the 9th Dist., Chairperson of the Committee on the part of the Senate, that the bill ought to pass.

AN ACT CONCERNING INSURANCE DATA AND INFORMATION SECURITY.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective October 1, 2019*) (a) This section may be cited as the "Insurance Data Security Law".

(b) The purpose of this section is to establish standards for data and information security for persons licensed and required to be licensed by the Insurance Commissioner, require licensees to notify the commissioner following cybersecurity events and require the commissioner to investigate such events.

(c) As used in this section:

(1) "Assuming insurer" means an insurer, including, but not limited to, an insurer that is a licensee, that acquires an insurance obligation or risk from a ceding insurer pursuant to an agreement between the insurers;

(2) "Authorized individual" means an individual who is known to, and screened by, a licensee, and to whom the licensee deems it necessary and appropriate to grant access to nonpublic information that is in the possession, custody or control of such licensee or stored on such licensee's information systems;

(3) "Ceding insurer" means an insurer, including, but not limited to, an insurer that is a licensee, that transfers an insurance obligation or risk to an assuming insurer pursuant to an agreement between the insurers;

(4) "Consumer" means an individual, including, but not limited to, an applicant, beneficiary, certificate holder, claimant, insured or policyholder, who is a resident of this state and whose nonpublic information is in the possession, custody or control of a licensee or stored on a licensee's information systems;

(5) "Cybersecurity event" means an event that involves unauthorized access to, or disruption or misuse of, a licensee's or third-party service provider's information systems or the nonpublic information stored thereon, except: (A) An event involving encrypted nonpublic information when the encryption process or encryption key is not acquired, released or used without authorization from the licensee or third-party service provider; or (B) if the licensee or third-party service provider determines that the person who accessed such nonpublic information (i) did not use or release such nonpublic information to a third party, and (ii) destroyed or returned such nonpublic information to such licensee or third-party service provider;

(6) "Encryption" means a process that transforms nonpublic information into a form that is unlikely to reveal the meaning of the nonpublic information without the use of a protective process or key;

(7) "Information security program" means a comprehensive written program that contains the administrative, physical and technical safeguards that a licensee uses to access, collect, dispose of, distribute, process, protect, store, transmit, use or otherwise handle nonpublic

information;

(8) "Information system" means: (A) A discrete set of electronic information resources organized for the collection, disposition, dissemination, maintenance, processing, sharing or use of electronic data or information; or (B) a specialized system, including, but not limited to, an environmental control system, industrial or process control system, or a telephone switching and private branch exchange system;

(9) "Licensee" means a person that is, or is required to be, authorized, licensed or registered in this state pursuant to title 38a of the general statutes, except: (A) For a purchasing group or risk retention group, as such terms are defined in section 38a-250 of the general statutes, that is chartered and licensed in another state; or (B) if such person is not domiciled in this state and is acting in such person's capacity as an assuming insurer;

(10) "Multifactor authentication" means a process that requires an individual to submit not less than two of the following forms of data or information to verify the individual's identity: (A) Information that is within the personal knowledge of such individual, including, but not limited to, a password; (B) electronic data or information that is within the possession, custody or control of such individual, including, but not limited to, a token or text message on a mobile telephone; or (C) data or information inherited by such individual, including, but not limited to, biometric data;

(11) "Nonpublic information" means data and information, other than public information and information concerning age or gender: (A) Concerning the business of a licensee that, if accessed, disclosed, tampered with or used without authorization from the licensee, would have a material adverse impact on the business, operations or security of such licensee; (B) that is in a form or medium created or derived from a consumer or health care provider concerning (i) the behavioral, mental or physical health of the consumer or a member of the family of such consumer, (ii) health care provided to the consumer, or (iii)

payment for health care provided to the consumer; or (C) concerning a consumer, including, but not limited to, the name, number, personal mark or other personal identifier of the consumer, that, in combination with any of the following forms of information, can be used to identify such consumer: (i) An access or security code, or a password, that would permit access to a financial account; (ii) an account, credit card or debit card number; (iii) biometric records; (iv) a driver's license number or an identification card number; or (v) a Social Security number;

(12) "Person" means an individual or a nongovernmental entity, including, but not limited to, a nongovernmental agency, association, branch, corporation or partnership;

(13) "Public information" means data or information that: (A) (i) Must be disclosed to the general public pursuant to applicable law, or (ii) may be made available to the general public from government records or widely distributed media; and (B) a licensee reasonably believes, after investigation, (i) is of a type that is available to the general public, and (ii) the consumer has not directed to be withheld from the general public, if the consumer may direct that such data or information be withheld from the general public pursuant to applicable law; and

(14) "Third-party service provider" means a person, other than a licensee, that: (A) Contracts with a licensee to maintain, process or store nonpublic information; or (B) is permitted to access nonpublic information while providing services to a licensee.

(d) (1) Not later than July 1, 2020, each licensee shall cause a risk assessment program to be implemented for such licensee that:

(A) Is continuously operated;

(B) Designates an affiliate, employee or outside vendor of such licensee as the person responsible for developing, implementing and maintaining the information security program for such licensee

pursuant to subdivision (1) of subsection (e) of this section;

(C) Identifies reasonably foreseeable threats, regardless of whether such threats originate inside or outside of such licensee, (i) that might result in unauthorized access to, or unauthorized alteration, destruction, disclosure, misuse or transmission of, nonpublic information that is in the possession, custody or control of such licensee, or (ii) to the security of such licensee's information systems and the nonpublic information that is accessible to, or in the possession, custody or control of, a third-party service provider that has contracted with such licensee;

(D) Assesses the likelihood of, and the potential damage resulting from, the reasonably foreseeable threats identified pursuant to subparagraph (C) of this subdivision, taking into account the sensitivity of the nonpublic information described in said subparagraph;

(E) Assesses the sufficiency of such licensee's information systems, and all policies, procedures and safeguards implemented to manage the reasonably foreseeable threats identified pursuant to subparagraph (C) of this subdivision, based on an assessment of, among other things, such licensee's policies, procedures and other safeguards concerning threats originating from such licensee's operations regarding (i) employee training and management, (ii) information systems, including, but not limited to, network design, software design and information classification, disposal, governance, processing, storage and transmission, and (iii) detection, prevention and response to cybersecurity events; and

(F) Implements information safeguards to (i) manage the reasonably foreseeable threats identified pursuant to subparagraph (C) of this subdivision, and (ii) at least annually, assess the effectiveness of the key controls, procedures and systems comprising such safeguards.

(2) Each licensee shall, on the basis of the risk assessment program implemented for such licensee pursuant to subdivision (1) of this

subsection:

(A) Include cybersecurity risks in such licensee's enterprise risk management process;

(B) Remain informed of emerging threats and vulnerabilities;

(C) Utilize security measures when sharing data or information that are reasonable in relation to the character of such sharing and the type of data or information shared;

(D) Provide all employees of such licensee with cybersecurity awareness training that is updated, on an ongoing basis, to account for all risks identified in such risk assessment program; and

(E) Determine whether the security measures set forth in subparagraphs (E)(i) to (E)(xii), inclusive, of this subdivision are appropriate, and, if such licensee determines that such security measures are appropriate, implement such security measures:

(i) Access control measures for such licensee's information systems, including, but not limited to, measures that authenticate the identities of, and restrict access to, authorized individuals;

(ii) Measures that identify and manage data, devices, facilities, personnel and systems and enable such licensee to achieve such licensee's business purposes in accordance with the relative importance of such purposes to such licensee's business objectives and risk strategy;

(iii) Measures that restrict, to authorized individuals, access to physical locations containing nonpublic information;

(iv) Measures that protect, by encryption or other means, nonpublic information while such nonpublic information is transmitted over an external network or stored on a laptop computer or other portable computing device, storage device or medium;

(v) Secure development measures for software applications

developed and utilized by such licensee;

(vi) Measures for assessing, evaluating and testing the security of software applications utilized but not developed by such licensee;

(vii) Measures to modify such licensee's information systems in accordance with the information security program developed, implemented and maintained for such licensee pursuant to subdivision (1) of subsection (e) of this section;

(viii) Effective control measures, including, but not limited to, multifactor authentication, for individuals accessing nonpublic information;

(ix) Measures to regularly test and monitor such licensee's information systems and procedures to detect both actual and attempted attacks on, and intrusions into, such licensee's information systems;

(x) Measures to include audit trails within the information security program developed, implemented and maintained for such licensee pursuant to subdivision (1) of subsection (e) of this section to (I) detect and respond to cybersecurity events, and (II) reconstruct material financial transactions in a manner that is sufficient to support such licensee's normal operations and obligations;

(xi) Measures to protect against damage or destruction to, or loss of, nonpublic information caused by environmental hazards, including, but not limited to, fire and water, other catastrophes or technological failures; and

(xii) Measures to dispose of nonpublic information regardless of the format of such nonpublic information.

(e) (1) Not later than October 1, 2020, each licensee shall cause an information security program to be developed, implemented and maintained for such licensee that:

(A) Is commensurate with the (i) complexity and size of such licensee, (ii) nature and scope of such licensee's activities, including, but not limited to, such licensee's use of third-party service providers, and (iii) sensitivity of the nonpublic information that is used by, or in the possession, custody or control of, such licensee or stored on such licensee's information systems;

(B) Is based on the risk assessment program implemented for such licensee pursuant to subdivision (1) of subsection (d) of this section;

(C) Is designed to (i) protect against hazards or threats to the (I) integrity and security of such licensee's information systems, and (II) confidentiality and security of the nonpublic information that is in the possession, custody or control of such licensee, and (ii) minimize the likelihood of harm to consumers resulting from any unauthorized access to, or use of, the nonpublic information that is in the possession, custody or control of such licensee;

(D) Establishes, and provides for the periodic reevaluation of, a schedule for the retention of the nonpublic information that is used by, or in the possession, custody or control of, such licensee or stored on such licensee's information systems, and a mechanism for the destruction of such nonpublic information when such licensee no longer requires such nonpublic information; and

(E) Includes a written incident response plan that (i) is designed to promptly respond to, and recover from, each cybersecurity event that compromises (I) such licensee's information systems, (II) the continued functioning of any aspect of such licensee's business operations, or (III) the availability, confidentiality or integrity of the nonpublic information that is in the possession, custody or control of such licensee, (ii) addresses such licensee's internal processes for responding to cybersecurity events, (iii) sets forth the goals of such plan, (iv) clearly defines the various responsibilities, roles and levels of decision-making authority concerning cybersecurity events, (v) addresses both internal and external communications and information sharing, (vi) identifies requirements for the remediation of any weaknesses

identified in such licensee's information systems or the controls associated with such information systems, (vii) provides for the documentation and reporting of cybersecurity events and any activities undertaken in response to cybersecurity events, and (viii) establishes a process to evaluate and, if necessary, revise such plan following each cybersecurity event.

(2) Each licensee shall evaluate, monitor and adjust the information security program developed, implemented and maintained for such licensee pursuant to subdivision (1) of this subsection in a manner that is consistent with:

(A) Relevant changes in technology;

(B) The sensitivity of the nonpublic information that is in the possession, custody or control of such licensee or stored on such licensee's information systems;

(C) Threats to the nonpublic information described in subparagraph (B) of this subdivision, regardless of whether such threats originate inside or outside of such licensee;

(D) Changes in the arrangement of such licensee's business, including, but not limited to, acquisitions, alliances, joint ventures, mergers and outsourcing; and

(E) Changes in such licensee's information systems.

(3) (A) If a licensee is governed by a board of directors, such board, or a committee of such board, shall, at a minimum, require the executive management of the licensee, or a person designated by such executive management, to:

(i) Cause an information security program to be developed, implemented and maintained for such licensee pursuant to subdivision (1) of this subsection; and

(ii) Report, at least annually, to such board concerning (I) the overall

status of the information security program developed, implemented and maintained for such licensee pursuant to subdivision (1) of this subsection, and (II) all matters material to such information security program, including, but not limited to, control decisions, cybersecurity events and responses thereto, recommendations for changes to such information security program, the ongoing risk assessment program implemented for such licensee pursuant to subdivision (1) of subsection (d) of this section, risk management measures, testing results and third-party service provider arrangements.

(B) If the executive management of a licensee designates a person that is not a member of such executive management to perform the responsibilities established in subparagraph (A) of this subdivision, such executive management shall:

(i) Oversee the development, implementation and maintenance by such person of an information security program for such licensee pursuant to subdivision (1) of this subsection; and

(ii) Require that such person submit a report, at least annually, to such executive management containing the information set forth in subparagraph (A)(ii) of this subdivision.

(4) Not later than October 1, 2021, each licensee shall require each third-party service provider that contracts with such licensee, or is permitted to access nonpublic information that is in the possession, custody or control of such licensee or stored on such licensee's information systems, to implement appropriate administrative, physical and technical measures to protect and secure all information systems that are, and all nonpublic information that is, accessible to or held by such third-party service provider. Each licensee shall exercise due diligence in selecting third-party service providers.

(f) Not later than February 15, 2021, and annually thereafter, each insurer domiciled in this state shall submit to the Insurance Commissioner, in a form and manner prescribed by the commissioner, a written statement certifying that such insurer is in compliance with

the provisions of subsections (d) and (e) of this section. Each insurer domiciled in this state shall maintain, for a period of not less than five years from the date such insurer submits a written statement to the commissioner pursuant to this subsection, all data, information, records and schedules supporting such written statement. If an insurer domiciled in this state identifies areas, processes or systems that require material improvements, redesign or updates, the insurer shall document and identify all remediation efforts, whether such efforts are planned or underway, to address such areas, processes or systems. Each insurer domiciled in this state shall, upon demand by the commissioner, make available to the commissioner all written statements and documents that such insurer is required to maintain pursuant to this subsection.

(g) (1) Beginning on October 1, 2020, each third-party service provider that discovers that a cybersecurity event involving such third-party service provider's information systems has occurred shall, in a form and manner prescribed by the Insurance Commissioner and in no event later than seventy-two hours after discovering such cybersecurity event, notify each licensee that has contracted with such third-party service provider and is affected by such cybersecurity event, or each person designated to act on behalf of a licensee, that such cybersecurity event has occurred.

(2) (A) Except as provided in subparagraph (B) of this subdivision, if a licensee suspects that a cybersecurity event involving the licensee's information systems has occurred, such licensee, or a person designated to act on behalf of such licensee, shall promptly conduct an investigation to, at a minimum, determine whether the suspected cybersecurity event occurred, and, if the suspected cybersecurity event occurred:

(i) Assess the nature and scope of such cybersecurity event;

(ii) Identify all nonpublic information that might have been involved in such cybersecurity event; and

(iii) Perform, or oversee the implementation of, reasonable measures to (I) restore the security of such information systems, and (II) prevent further unauthorized acquisition, release or use of the nonpublic information that is stored on such information systems.

(B) If a third-party service provider notifies a licensee, or a person designated to act on behalf of a licensee, pursuant to subdivision (1) of this subsection that the third-party service provider has discovered that a cybersecurity event involving such third-party service provider's information systems has occurred, or if a licensee has actual knowledge that such a cybersecurity event has occurred, the licensee shall:

(i) Confirm, and maintain records confirming, that such third-party service provider promptly conducted an investigation that satisfies the requirements established in subparagraph (A) of this subdivision; or

(ii) Promptly conduct an investigation that satisfies the requirements established in subparagraph (A) of this subdivision on behalf of such third-party service provider.

(3) (A) Except as provided in subparagraph (B) of this subdivision, each licensee, or a person designated to act on behalf of such licensee, shall promptly notify the commissioner, in a form and manner prescribed by the commissioner and in no event later than the applicable deadline established in subdivision (4) of this subsection, that a cybersecurity event has occurred if:

(i) Such licensee is (I) an insurer, as defined in section 38a-1 of the general statutes, that is domiciled in this state, or (II) an insurance producer whose home state, as such terms are defined in section 38a-702a of the general statutes, is this state; or

(ii) Such licensee reasonably believes that the nonpublic information involved in such cybersecurity event concerns not less than two hundred fifty consumers, and (I) such licensee is required to send notice concerning such cybersecurity event to any government body,

self-regulatory agency or supervisory body pursuant to any applicable federal or state law, or (II) it is reasonably likely that such cybersecurity event will materially harm any consumer or any material part of the normal operations of such licensee.

(B) Each licensee acting in such licensee's capacity as an assuming insurer, or a person designated to act on behalf of such licensee, shall promptly notify the commissioner and each ceding insurer affected by a cybersecurity event, in a form and manner prescribed by the commissioner and in no event later than the deadline established in subdivision (4) of this subsection, that a cybersecurity event has occurred if:

(i) The cybersecurity event involves nonpublic information that (I) comes into the possession, custody or control of, or involves information systems maintained by, such licensee in such licensee's capacity as an assuming insurer, or (II) is stored on the information systems of a third-party service provider that contracted with such licensee in such licensee's capacity as an assuming insurer;

(ii) Such licensee reasonably believes that the criteria established in subparagraph (A)(ii) of this subdivision are satisfied; and

(iii) Such licensee does not have a direct contractual relationship with the consumers affected by such cybersecurity event.

(4) Each licensee, or person designated to act on behalf of a licensee, that is required to send notice to the commissioner pursuant to subparagraph (A) of subdivision (3) of this subsection, or the commissioner and a ceding insurer pursuant to subparagraph (B) of said subdivision, shall send such notice to the commissioner, or the commissioner and a ceding insurer, as applicable, not later than seventy-two hours after:

(A) Such licensee, or the person designated to act on behalf of such licensee, first discovers a cybersecurity event if the cybersecurity event involves information systems maintained by such licensee; or

(B) Such licensee, or the person designated to act on behalf of such licensee, receives notice from a third-party service provider pursuant to subdivision (1) of this subsection disclosing that a cybersecurity event has occurred, or such licensee first has actual knowledge that a cybersecurity event involving the information systems maintained by a third-party service provider has occurred.

(5) Each licensee, or person designated to act on behalf of such licensee, that notifies the commissioner pursuant to subparagraph (A) of subdivision (3) of this subsection or receives notice from an assuming insurer pursuant to subparagraph (B) of said subdivision shall, not later than the deadline established in subdivision (4) of this subsection and in an electronic form prescribed by the commissioner, submit the following information to the commissioner, if and to the extent that such information is available to such licensee or person, and shall supplement and update such information as additional information becomes available:

(A) The date of the cybersecurity event;

(B) A description of how the nonpublic information involved in the cybersecurity event was breached, exposed, lost or stolen, including, but not limited to, a description of the specific responsibilities and roles of each third-party service provider involved in the cybersecurity event;

(C) How the cybersecurity event was discovered;

(D) Whether any nonpublic information involved in the cybersecurity event was recovered and, if such nonpublic information was recovered, how such nonpublic information was recovered;

(E) The identity of each person who perpetrated the cybersecurity event;

(F) Whether such licensee, or person designated to act on behalf of such licensee, notified any government, law enforcement or regulatory agency, other than the commissioner, regarding the cybersecurity

event and, if so, when such licensee, or person designated to act on behalf of such licensee, issued such notice;

(G) A description of each specific type of nonpublic information involved in the cybersecurity event, including, but not limited to, financial or medical information;

(H) The period during which each information system involved in the cybersecurity event was compromised by such cybersecurity event;

(I) The number of consumers affected by the cybersecurity event or, if such number is unavailable, the best estimate of the number of consumers affected by such cybersecurity event;

(J) The results of any review conducted by such licensee, or person designated to act on behalf of such licensee, that (i) identifies any lapse in the automated controls or internal procedures of such licensee, or (ii) confirms that all automated controls and internal procedures of such licensee were followed;

(K) A description of any efforts undertaken to remediate the conditions that caused or enabled the cybersecurity event;

(L) A copy of any privacy policy implemented by or for such licensee;

(M) A statement outlining all steps that such licensee, or person designated to act on behalf of such licensee, will take to (i) investigate the cybersecurity event, and (ii) notify all consumers affected by the cybersecurity event;

(N) The name of an individual, designated by such licensee or person designated to act on behalf of such licensee, who is (i) familiar with the cybersecurity event, and (ii) authorized to act on behalf of such licensee; and

(O) If such licensee is subject to the notice requirement established in subparagraph (A) of subdivision (6) of this subsection, a copy of the

notice that such licensee sent to residents of this state, owners and licensees pursuant to section 36a-701b of the general statutes.

(6) Each licensee, or person designated to act on behalf of a licensee, that is required to send notice to the commissioner following a cybersecurity event pursuant to subparagraph (A) of subdivision (3) of this subsection, and each ceding insurer who receives notice from an assuming insurer following a cybersecurity event pursuant to subparagraph (B) of said subdivision and maintains a direct contractual relationship with the consumers affected by the cybersecurity event, shall:

(A) Notify the consumers affected by the cybersecurity event in the manner specified in section 36a-701b of the general statutes; and

(B) If a consumer affected by the cybersecurity event accessed such licensee's services through an insurance producer, as defined in section 38a-702a of the general statutes, and such licensee has the current contact information for the insurance producer, notify such insurance producer at a time and in a manner prescribed by the commissioner.

(h) Beginning on October 1, 2020, each licensee shall maintain records concerning each cybersecurity event for a period of not less than five years from the date of the cybersecurity event.

(i) (1) Beginning on October 1, 2020, whenever the Insurance Commissioner has reason to believe that a licensee has violated any provision of this section, the commissioner shall:

(A) Have the power to examine and investigate the affairs of the licensee, in the manner set forth in sections 38a-14 to 38a-16, inclusive, of the general statutes and in compliance with this section, to determine whether such licensee has violated such provision; and

(B) Issue and serve upon the licensee a (i) statement setting forth such violation, and (ii) notice of a hearing to be held at a time and place fixed in such notice, which time shall not be less than thirty calendar days after the date of service of such notice.

(2) (A) A licensee shall, at the time and place fixed for a hearing in a notice issued and served upon the licensee pursuant to subparagraph (B) of subdivision (1) of this subsection, have an opportunity to be heard and show cause why an order should not be entered by the commissioner (i) enforcing the provisions of this section, or (ii) suspending, revoking or refusing to reissue or renew any license, certificate of registration or authorization to operate the commissioner has issued, or may issue, to such licensee.

(B) The commissioner may, after holding a hearing pursuant to subparagraph (A) of this subdivision and in addition to or in lieu of suspending, revoking or refusing to reissue or renew any license, certificate of registration or authorization to operate the commissioner has issued, or may issue, to a licensee, impose on the licensee a civil penalty of not more than fifty thousand dollars for each violation of any provision of this section. The commissioner may bring a civil action to recover the amount of any civil penalty the commissioner imposes on a licensee pursuant to this subparagraph.

(3) (A) Except as provided in subparagraph (B) of this subsection:

(i) All documents, information and materials that a licensee submits to the commissioner pursuant to subparagraphs (B), (C), (D), (E), (H), (J) and (K) of subdivision (5) of subsection (g) of this section, or that the commissioner obtains in connection with an investigation conducted pursuant to subparagraph (A) of subdivision (1) of this subsection, shall (I) be confidential and privileged, (II) not be subject to disclosure under the Freedom of Information Act, as defined in section 1-200 of the general statutes or any subpoena or discovery in any private cause of action, and (III) not be introduced into evidence in any private cause of action; and

(ii) The commissioner and all persons acting on behalf of the commissioner who receive any document, information or material described in subparagraph (A)(i) of this subdivision shall not be permitted or compelled to testify in any private cause of action concerning such document, information or material.

(B) The commissioner may:

(i) Exercise the commissioner's authority in any legal or regulatory action, or use any document, information and material described in subparagraph (A)(i) of this subdivision in furtherance of such action;

(ii) Submit documents, information and materials, including, but not limited to, documents, information and materials described in subparagraph (A)(i) of this subdivision, to the Attorney General, other state, federal or international regulatory agencies and law enforcement authorities, and the National Association of Insurance Commissioners and the affiliates and subsidiaries of such association, provided the recipient of such documents, information and materials agrees, in writing, to maintain such documents, information and materials as confidential in a manner that satisfies the requirements established in subparagraph (A) of this subdivision;

(iii) Receive documents, information and materials, including, but not limited to, confidential or privileged documents, information and materials, from the Attorney General, other state, federal or international regulatory agencies and law enforcement authorities, and the National Association of Insurance Commissioners and the affiliates and subsidiaries of such association, provided the commissioner agrees, in writing, to treat such documents, information and materials as if such documents, information and materials were submitted to the commissioner in the manner described in subparagraph (A)(i) of this subdivision;

(iv) Submit documents, information and materials described in subparagraph (A)(i) of this subdivision to a third-party consultant or vendor, provided the consultant or vendor agrees, in writing, to treat such documents, information and materials as confidential in a manner that satisfies the requirements of subparagraph (A) of this subdivision;

(v) Enter into agreements governing the submission, receipt and use of documents, information and materials in a manner that satisfies the

requirements established in this subdivision; and

(vi) Notwithstanding any contrary provision in this subdivision, release to any clearinghouse service or database maintained by the National Association of Insurance Commissioners, or any affiliate or subsidiary of such association, a final, adjudicated action that is subject to disclosure under the Freedom of Information Act, as defined in section 1-200 of the general statutes.

(C) No waiver of any applicable privilege or claim of confidentiality in any document, information or material shall occur as a result of any submission made to, or receipt by, the commissioner of such document, information or material in the manner described in subparagraphs (A) and (B) of this subdivision.

(j) (1) Notwithstanding any contrary provision in this section:

(A) Each licensee that has fewer than ten employees or independent contractors shall not be subject to the requirements established in subsections (d) to (f), inclusive, of this section;

(B) Each licensee that is subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as amended from time to time, and establishes and maintains an information security program that satisfies all applicable provisions of such act and the guidelines, procedures, regulations and rules promulgated thereunder shall be deemed to have satisfied the requirements established in subsections (d) to (f), inclusive, of this section, provided such licensee files with the Insurance Commissioner, in a form and manner prescribed by the commissioner, a certification that such licensee is in compliance with such provisions; and

(C) Each licensee that is an agent, designee, employee or representative of any other licensee shall not be subject to the requirements established in subsections (d) to (f), inclusive, of this section, and shall not be required to cause an information security program to be developed, implemented and maintained for such

agent, designee, employee or representative pursuant to subsection (e) of this section, provided such agent, designee, employee or representative is covered by the information security program developed, implemented and maintained for such other licensee.

(2) Each licensee that ceases to qualify for an exception under subdivision (1) of this subsection shall comply with all provisions of this section that apply to such licensee not later than one hundred eighty days after such licensee no longer qualifies for such exception.

(k) Nothing in this section shall be construed to create a private right of action, or to affect or limit a private right of action that exists without regard to this section.

(l) The Insurance Commissioner may adopt such regulations, in accordance with chapter 54 of the general statutes, to implement the provisions of this section.

Sec. 2. Subparagraph (B) of subdivision (2) of subsection (b) of section 36a-701b of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2020*):

(B) The person who conducts business in this state, and who, in the ordinary course of such person's business, owns or licenses computerized data that includes personal information, shall offer to each resident whose **[**personal**]** nonpublic information under subparagraph **[**(A)**]** (C)(v) of subdivision **[**(4)**]** (11) of subsection **[**(a)**]** (c) of section **[**38a-999b**]** 1 of this act or personal information as defined in subparagraph (A) of subdivision (2) of subsection (a) of this section was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twenty-four months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file.

Sec. 3. Section 38a-999b of the general statutes is repealed. (*Effective October 1, 2020*)

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2019*	New section
Sec. 2	*October 1, 2020*	36a-701b(b)(2)(B)
Sec. 3	*October 1, 2020*	Repealer section

INS *Joint Favorable*

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact:

Agency Affected	Fund-Effect	FY 20 $	FY 21 $
Insurance Dept.	GF - Potential Revenue Gain	None	Minimal

Note: GF=General Fund

Municipal Impact: None

Explanation

The bill updates and expands the state's insurance data security law, placing requirements on licensees and authorizing the insurance commissioner to enforce its provisions. There is no cost anticipated for the Insurance Department. To the extent the commissioner imposes civil penalties permitted under the bill beginning in FY 21, up to $50,000 for each violation, there is a potential minimal revenue gain to the General Fund.

The Out Years

The annualized ongoing potential fiscal impact identified above will continue into the future.

Sources: Connecticut Insurance Department

OLR Bill Analysis

SB 903

AN ACT CONCERNING INSURANCE DATA AND INFORMATION SECURITY.

SUMMARY

This bill repeals the state's information security program law, replacing it with provisions substantially similar to the National Association of Insurance Commissioners (NAIC) insurance data security model law.

Current law requires insurers, pharmacy benefit managers (PBMs), third-party administrators (TPAs), utilization review companies, and any other entity licensed to do health insurance business to implement and maintain a written comprehensive information security program to safeguard the personal information of insureds and enrollees. Among other things, the program must be appropriate to the business' size, scope, type, available resources, and data, and the type of security and confidentiality necessary.

The bill generally incorporates current law's information security provisions as they relate to data security breaches, access control measures, investigations, reporting, and oversight. However, the bill's requirements are more comprehensive and apply to all entities licensed under the insurance statutes, excluding a purchasing or risk retention group chartered in another state and nondomiciled assuming insurers. The bill also protects consumers' "nonpublic information," not just personal information under current law. Specifically the bill:

1. requires licensees to develop a risk assessment program, investigate cybersecurity events, and notify the insurance commissioner of any such event within 72 hours;

2. authorizes the commissioner to enforce its provisions; fine violators up to $50,000; and adopt implementing regulations; and

3. applies existing law's identity theft mitigation and data breach security requirements to all licensees as it related to the breach of consumers' nonpublic information.

The bill defines "nonpublic information" as information that is not public, not related to age or gender, and that (1) would materially impact a licensee's business, operation, or security if disclosure, (2) is created or derived from a consumer or health care provider and concerns behavioral, mental, or physical health or health care services or payments, or (3) concerns a consumer's name, number, or other personal identifiable information that can identify a consumer when used in combination with an access or security code; account, credit or debit card number; biometric records; driver's license or identification number; or Social Security number.

Under the bill, a "cybersecurity event" is unauthorized access to information systems or nonpublic information.

EFFECTIVE DATE: October 1, 2019, for the provisions related to the new Insurance Data Security Law (§ 1); October 1, 2020, for the provisions related to existing identity theft mitigation services requirements (§ 2); and October 1, 2020, for the repeal of the current Comprehensive Information Security Program law (§ 3).

§ 1 — NEW INSURANCE DATA SECURITY LAW

The bill requires licensees to:

1. develop and implement risk assessment and information security programs to protect nonpublic information; and

2. along with certain third-party service providers (i.e., entities that can access or are contracted with a licensee to maintain, process, or store nonpublic information) investigate cybersecurity events

and, within 72 hours, report any such event to the commissioner.

(These provisions are effective October 1, 2019, and require implementation of the risk assessment program by July 1, 2020. The bill repeals and replaces the current information security program requirements on October 1, 2020, thus resulting in a three-month period during which both sets of program requirements apply.)

Risk Assessment Program

Program Requirements. The bill requires each licensee to implement a continuously operated risk assessment program by July 1, 2020, that:

1. designates an affiliate, employee, or outside vendor to develop, implement, and maintain an information security program;

2. identifies reasonably foreseeable internal and external threats (a) that might result in unauthorized access or alteration, destruction, disclosure, misuse, or transmission of nonpublic information held by the licensee or (b) to the licensee's security information systems and nonpublic information in possession, custody, or control of, or accessible to, a third-party service provider;

3. assesses the likelihood and potential damage of reasonably foreseeable threats, taking into account the sensitivity of any nonpublic information; and

4. implements information safeguards, including key controls, procedures, and systems, to manage reasonably foreseeable threats and assess them at least annually.

The risk assessment program must also assess the sufficiency of the licensee's information system and all policies, procedures, and safeguards to manage against reasonably foreseeable threats that might originate from the licensee's operation (e.g., internal threats). This assessment must include (1) employee training and management;

(2) information systems, including network and software design, and information classification, disposal, governance, processing, storage, and transmission; and (3) detection, prevention, and response to cyber security events.

Post-Implementation. The bill also requires each licensee, on the basis of the risk assessment program, to:

1. include cybersecurity risks in their enterprise risk management process;

2. remain informed of emerging threats and vulnerabilities;

3. utilize reasonable security measures relative to the data's type and sensitivity when sharing it; and

4. provide employees with up-to-date and ongoing cybersecurity awareness training that accounts for all risks the assessment program identifies.

Security Measures. Licensees must also determine and implement the following security measures, as appropriate:

1. access control measures for information systems, including ways to identify and restrict access to authorized individuals;

2. measures that identify and manage data, device, facilities, personnel, and systems as appropriate to the licensee's business;

3. measures that restrict access to physical locations containing nonpublic information to authorized individuals;

4. measures that protect, by encryption or other means, nonpublic information while it is being transmitted over an external network or stored on a laptop or other portable device;

5. secures development measures for software applications the licensee develops and uses;

6. measures for assessing, evaluating, and testing the security of software applications the licensee uses that were developed by someone else;

7. measures to modify the licensee's information systems in accordance with its information security program (see below);

8. effective control measures, including multifactor authentication for individuals accessing nonpublic information;

9. measures to include audit trails within the information security program to detect and respond to cybersecurity events and reconstruct material financial transactions;

10. measures to regularly rest and monitor the information systems and procedures to detect both actual and attempted attacks;

11. measures to protect against damage or destruction, or loss of nonpublic information caused by environmental hazards, including fire, water, catastrophes, or technological failures; and

12. measures to dispose of nonpublic information regardless of its format.

Information Security Program

Plan Design. The bill requires licensees, by October 1, 2020, to develop, implement, and maintain an information security program based on the risk assessment program described above that:

1. is commensurate with the (a) licensee's complexity, size, nature, and business scope, including any use of third-party service providers and (b) sensitivity of the nonpublic data used by, or in possession or control of, the licensees information systems; and

2. establishes and provides for periodic reevaluation of a nonpublic data retention schedule and a mechanism for destroying it once the licensee is done using the data.

The plan must be designed to:

1. protect against hazards or threats to the (a) integrity and security of the licensee's information systems and (b) confidentiality and security of nonpublic information held or controlled by the licensee and

2. minimize the likelihood of harm to consumers resulting from any unauthorized access to, or use of, nonpublic information.

Written Incident Response Plan. The plan must also include a written incident response plan that:

1. is designed to promptly respond to, and recover from, cybersecurity events that compromise a licensee's information systems, business operations, or the confidentiality, availability, or integrity of nonpublic information it holds;

2. addresses the licensee's internal response process to cybersecurity events, including clearly defining the responsibilities, roles, and levels of decision making authority;

3. establishes goals for the plan;

4. addresses both internal and external communications and information sharing;

5. identifies requirements for remediating any weakness in the licensee's information systems or controls;

6. provides for the documenting and reporting of cybersecurity events and response activities; and

7. establishes a process to evaluate and if necessary revise the plan.

Plan Evaluation. Under the bill, each licensee must evaluate, monitor, and adjust the information security program consistent with:

1. relevant technological changes;

2. the sensitivity of the nonpublic information;

3. threats to nonpublic information, regardless of where they originate;

4. changes in a licensee's business arrangements, including acquisitions, alliances, joint ventures, mergers, and outsources; and

5. changes in licensee information systems.

Board of Directors Requirements. If a licensee is governed by a board of directors, the board or one of its committees must require the licensee's executive management or a designee to develop, implement, and maintain the information security program and report at least annually to the board about the program's status and related matters. This must include control decisions, cybersecurity events and responses, recommended changes, the ongoing risk assessment, testing results, and any arrangements with third-party providers.

If the executive management designates an individual who is not in an executive management role to perform these responsibilities, the bill requires the executive management to oversee the development, implementation, and maintenance of the program and require that the designee report to it with the same information described above that must be reported to the board.

Third Party Service Provider Contracts

By October 1, 2021, the bill requires licensees that contract with third-party service providers or allow them access to their nonpublic information to implement appropriate administrative, physical, and technical measures to protect and secure all nonpublic information that they hold or to which they have access. Under the bill, each licensee must exercise due diligence in selecting third-party service providers.

Certification to Commissioner and Record Retention Requirements

Annually, starting by February 15, 2021, the bill requires domestic

insurers to submit to the insurance commissioner, in a form and manner he prescribes, a written statement certifying that the insurer has complied with the bill's risk assessment and information security program provision. Each domestic insurer must maintain all supporting documents, including data, information, records, and schedules, for at least five years after submitting its certification.

The bill also requires a domestic insurer that identifies areas, process, or systems that require material improvements, redesigns, or updates to document and identify the remediation efforts planned and underway and make such documents available to the commissioner on request.

Beginning October 1, 2020, the bill requires each licensee to retain records of cybersecurity events for at least five years after the event occurs.

72-Hour Reporting Requirement

The bill establishes notification requirements for licensees and third-party service providers following cybersecurity events.

Licensees. Under the bill, each licensee must notify the commissioner, in a form and manner he prescribes, within 72 hours of a cybersecurity event if the licensee:

1. is an insurer domiciled in the state (i.e., a domestic insurer) or an insurance producer whose home state is Connecticut or

2. reasonably believes the nonpublic information involved in the cybersecurity event effects 250 people or more and (a) the licensee is required to send a cybersecurity notice to any governing, regulatory, or supervisory body under federal or state law or (b) it is reasonably likely the cybersecurity event will materially harm any consumer or the licensee's business.

If a licensee is acting as an assuming insurer (i.e., an insurer that acquires an insurance obligation from another insurer), it must notify

the commissioner and the ceding insurer (i.e., the insurer that transferred the obligations) within 72 hours if the cybersecurity event involves nonpublic information that is (1) possessed, controlled, or involves information systems maintained by the licensee in its capacity as an assuming insurer or (2) stored on the information systems of a third-party service provider that contracts with the licensee in its capacity as an assuming insurer.

Third-Party Service Providers. Under the bill, on and after October 1, 2020, a third-party service provider that discovers a cybersecurity event on its own systems must notify, within 72 hours, each licensee it contracts with and that is affected by the event. The notification must be in a form and manner prescribed by the commissioner.

Notice to Commissioner

Any insurer that receives notice of a cybersecurity event from a third-party service provider or is required under the bill to notify the commissioner of an event must, in an electronic form prescribed by the commissioner, submit the following information and update it as new information becomes available:

1. the date the cybersecurity event occurred, how it was discovered, and the perpetrator's identity;

2. a description of how nonpublic information was breached, exposed, lost, or stolen, including the specific responsibilities and roles of any third-party service provider involved;

3. how much, if any, nonpublic information was recovered and how, and a description of the specific type of nonpublic information, including whether it was financial or medical information;

4. whether the licensee notified any government, law enforcement, or regulatory agency other than the insurance commissioner, and if so, when;

5. the period during which the information system was compromised and the number of consumers affected by the cybersecurity event, or the licensee's best estimate if the number is unavailable;

6. the results of any review the licensee conducted that (a) identifies lapses in automated controls or internal procedures or (b) confirms that all controls and procedures were followed;

7. a description of any efforts undertaken to remediate the conditions that caused the event and a copy of any privacy policy the licensee implemented or used;

8. a statement outlining all the steps the licensee will take to (a) investigate the event and (b) notify affected consumers;

9. the name of an individual familiar with the event and authorized to act on the licensee's behalf; and

10. a copy of any required notice to impacted consumers (see below).

Notice to Consumers

The bill requires (1) any insurer that notifies the commissioner of a cybersecurity event and (2) any ceding insurer who receives notice from an assuming insurer of an event and maintains a contractual relationship with impacted consumers to notify consumers within 90 days as required under existing law (CGS § 36a-701b).

If a consumer accessed affected services through an insurance producer, and the licensee has the producer's current contact information, the licensee must notify the producer of the event in a form and manner the commissioner prescribes.

Cybersecurity Event Investigations

The bill requires licensees that suspect a cybersecurity event involving its systems to promptly investigate and, at a minimum, determine whether the event occurred. If the licensee determines that

the event occurred, it must:

1. assess the event's nature and scope;

2. identify all nonpublic information that might have been involved; and

3. perform, or oversee implementing, reasonable procedures to restore system security and prevent further unauthorized acquisition, release, or use of nonpublic information.

If a licensee is notified by a third-party service provider of a cybersecurity event or otherwise has knowledge such an event has occurred, it must (1) immediately conduct an investigation as described above or (2) confirm, that the third-party service provider has conducted such an investigation and maintain records of such confirmation.

Enforcement

Beginning October 1, 2020, the bill requires the commissioner to enforce the bill's cybersecurity provisions and authorizes him to do so in accordance with his existing powers. It also requires him to issue and serve the licensee with a statement of the violation and notice of a hearing, to be held at least 30 days after the notice is served.

The licensee must have an opportunity to be heard and show cause why an order should not be entered by the commissioner enforcing the bill's provisions or suspending, revoking, or refusing to reissue or renew any license, registration, or authorization issued by the commissioner.

The commissioner may, after a hearing and in addition to or in lieu of actions he takes against the licensee's license, registration, or authorization, impose a civil penalty up to $50,000 for each violation. Under the bill, the commissioner may bring a civil action to recover any penalty imposed.

The bill allows the commissioner to exercise his authority in any

legal or regulatory action using any documents, information, and material submitted to, or obtained during an investigation by, the commissioner.

Confidentiality

The bill makes all documents submitted to or obtained by the commissioner during an investigation confidential and privileged. They are exempt from disclosure under the state's Freedom of Information Act (FOIA) and any subpoena or discovery in a private cause of action. The bill also prohibits such documents from being introduced as evidence in a private cause of action. It prohibits the commissioner and all persons acting on his behalf who receive confidential information from being allowed or compelled to testify in a private cause of action that concerns the confidential material.

He may submit such documents, information, and material to the (1) Attorney General or another state, federal, or international regulatory or law enforcement agency and (2) NAIC and its affiliates and subsidiaries, provided they agree in writing to maintain the same level of confidentiality. He may also (1) receive documents and information from these sources, provided he treats them as confidential, and (2) submit documents and information to third-party consultants or vendors, provided they agree in writing to maintain the documents' and information's confidentiality.

The commissioner may enter agreements governing the submission of documents, information, and materials in a way that maintains confidentiality.

Regardless of the bill's other provisions, it authorizes him to release to any NAIC clearinghouse or database a final adjudicated action that is subject to disclosure under FOIA.

The bill specifies that no waiver of any applicable privilege or claim of confidentiality in any document, information, or material occurs as a result of submitting it to, or it being received by, the commissioner.

Exemptions

The bill exempts independent contractors and licensees with nine or fewer employers from the risk assessment and information security program provisions, but still (1) requires them to report cybersecurity events under the bill's provisions and (2) extends the commissioner's enforcement authority over them.

Licensees subject to the federal Health Insurance Portability and Accountability Act that establish and maintain an information security program under the act are deemed to have satisfied the bill's risk assessment and information security program provisions. In such a case, the licensee must certify to the commissioner, in a form and manner he prescribes, that it complies with the federal law.

The bill also specifies that its provisions apply to licensees, and not their agents, designees, employees, or representatives, provided they are covered by the licensee's information security program. Licensees that cease to meet this exemption must comply with the bill's provisions within 180 days.

Private Right of Action

The bill specifies that it must not be construed to create a private right of action, or to affect or limit an existing private right of action.

§ 2 — EXISTING IDENTITY THEFT MITIGATION AND DATA BREACH SECURITY LAW

The bill adds "nonpublic information" to the state's data breach privacy laws. In doing so, starting October 1, 2020, it requires any person or business that owns or licenses computerized data that includes personal information to notify consumers if any of their nonpublic information has been breached or reasonably believed to have been breached and provide them up to two years of identity theft mitigation services, as is required under existing law regarding consumers' personal information. By law, personal information is an individual's first name or initial and last name with his or her (1) Social Security, driver's license, state identification number; (2) credit or debit

card number; or (3) financial account number in combination with a password that allows access to the account (CGS § 36a-701b).

COMMITTEE ACTION

Insurance and Real Estate Committee

Joint Favorable
Yea 19 Nay 0 (03/14/2019)