General Assembly

Raised Bill No. 5365

February Session, 2020

LCO No. **2175**

Referred to Committee on INSURANCE AND REAL ESTATE

Introduced by:
(INS)

AN ACT CONCERNING THE INSURANCE DEPARTMENT'S RECOMMENDATIONS REGARDING THE PUBLIC HEALTH FEE, THIRD PARTY PERFORMANCE OF THE DEPARTMENT'S EMPLOYEES' DUTIES, THE INSURANCE DATA SECURITY LAW AND ASSESSMENTS AGAINST DOMESTIC INSURANCE COMPANIES AND ENTITIES.

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

Section 1. Subsections (b) and (c) of section 19a-7p of the 2020 supplement to the general statutes are repealed and the following is substituted in lieu thereof (*Effective July 1, 2020*):

(b) (1) As used in this section: (A) "Health insurance" means health insurance of the types specified in subdivisions (1), (2), (4), (11) and (12) of section 38a-469; and (B) "health care center" has the same meaning as provided in section 38a-175.

(2) Each domestic insurer or domestic health care center doing health insurance business in this state shall annually pay to the Insurance Commissioner, for deposit in the Insurance Fund established under section 38a-52a, a public health fee assessed by the Insurance

Commissioner pursuant to this section.

(3) (A) Not later than September first, annually, each such insurer or health care center shall report to the Insurance Commissioner, in the form and manner prescribed by **[**said**]** the commissioner, the number of insured or enrolled lives in this state as of May first immediately preceding the date for which such insurer or health care center is providing health insurance that provides coverage of the types specified in subdivisions (1), (2), (4), (11) and (12) of section 38a-469. Such number shall not include lives enrolled in Medicare, any medical assistance program administered by the Department of Social Services, workers' compensation insurance or Medicare Part C plans. The commissioner may require each such insurer or health care center or any other person to submit to the commissioner any records that are in such insurer's, health care center's or other person's possession if such records were used to prepare such insurer's or health care center's annual report submitted pursuant to this subparagraph.

(B) Each such insurer or health care center that fails to timely submit an annual report pursuant to subparagraph (A) of this subdivision shall pay to the Insurance Commissioner, in the form and manner prescribed by the commissioner, a late filing fee of one hundred dollars per day for each day from the date that the annual report was due.

(C) If the Insurance Commissioner determines that there is a discrepancy, other than a good faith discrepancy, between the number of insured or enrolled lives that the insurer or health care center reported to the commissioner pursuant to subparagraph (A) of this subdivision and the number of such lives that the insurer or health care center should have reported to the commissioner pursuant to said subparagraph (A), the insurer or health care center shall be liable for a civil penalty of not more than fifteen thousand dollars.

(c) Not later than November first, annually, the Insurance Commissioner shall determine the fee to be assessed for the current fiscal year against each such insurer and health care center. Such fee

shall be calculated by multiplying the number of lives reported to said commissioner pursuant to subparagraph (A) of subdivision (3) of subsection (b) of this section by a factor, determined annually by said commissioner as set forth in this subsection, to fully fund the aggregate amount determined under subsection (a) of this section. The Insurance Commissioner shall determine the factor by dividing the aggregate amount by the total number of lives reported to said commissioner pursuant to subparagraph (A) of subdivision (3) of subsection (b) of this section.

Sec. 2. Subsection (d) of section 38a-8 of the 2020 supplement to the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2020*):

(d) The commissioner shall develop a program of periodic review to ensure compliance by the Insurance Department with the minimum standards established by the National Association of Insurance Commissioners for effective financial surveillance and regulation of insurance companies operating in this state. The commissioner shall adopt regulations, in accordance with the provisions of chapter 54, pertaining to the financial surveillance and solvency regulation of insurance companies and health care centers as are reasonable and necessary to obtain or maintain the accreditation of the Insurance Department by the National Association of Insurance Commissioners. The commissioner shall maintain as confidential any confidential documents or information received from the National Association of Insurance Commissioners, or the International Association of Insurance Supervisors, or any documents or information received from state or federal insurance, banking or securities regulators or similar regulators in a foreign country that are confidential in such jurisdictions. The commissioner may share any information, including confidential information, with the National Association of Insurance Commissioners, the International Association of Insurance Supervisors, or state or federal insurance, banking or securities regulators or similar regulators in a foreign country, provided the commissioner determines that such entities agree to maintain the same level of confidentiality in

their jurisdictions as is available in this state. At the expense of a domestic, alien or foreign insurer, the commissioner may engage the services of attorneys, actuaries, accountants and other experts not otherwise part of the commissioner's staff as may be necessary to assist the commissioner in the financial analysis of the insurer, the review of the insurer's license applications, and the review of transactions within a holding company system involving an insurer domiciled in this state. **[**No duties of a person employed by the Insurance Department on November 1, 2002, shall be performed by such attorney, actuary, accountant or expert.**]**

Sec. 3. Subsections (b) to (g), inclusive, of section 38a-38 of the 2020 supplement to the general statutes are repealed and the following is substituted in lieu thereof (*Effective October 1, 2020*):

(b) Definitions. For the purposes of this section:

(1) "Authorized individual" means an individual who is known to, and screened by, a licensee, and who is determined to be necessary and appropriate to have access to the nonpublic information that is held by the licensee and on such licensee's information systems.

(2) "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 a licensee's possession, custody or control.

(3) "Cybersecurity event" means an event resulting in any unauthorized access to, or disruption or misuse of, an information system or the nonpublic information stored thereon, except if: (A) The event involves the unauthorized acquisition of encrypted nonpublic information if the encryption process for such information or encryption key to such information is not acquired, released or used without authorization; or (B) the event involves access of nonpublic information by an unauthorized person and the licensee determines that such information has not been used or released and has been returned or destroyed.

(4) "Encryption" means the transformation of data or information into a form that results in a low probability of assigning meaning to such data or information without the use of a protective process or key.

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

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

(7) "Licensee" means any person licensed, authorized to operate or registered, or required to be licensed, authorized to operate or registered, pursuant to the insurance laws of this state, **[**except for**]** including, but not limited to, a fraternal benefit society, an interlocal risk management agency formed pursuant to chapter 113a or an employers' mutual association authorized under part C of chapter 568, but not including a purchasing group or **[**a**]** risk retention group chartered and licensed in another state, **[**or**]** a **[**licensee that is**]** person acting as an assuming insurer and domiciled in another state or jurisdiction or a commissioner of the Superior Court acting as a title agent, as defined in section 38a-402.

(8) "Multifactor authentication" means authentication through verification of at least two of the following types of authentication factors: (A) A knowledge factor, including, but not limited to, a password; (B) a possession factor, including, but not limited to, a token or text message on a mobile phone; or (C) an inheritance factor, including, but not limited to, a biometric characteristic.

(9) "Nonpublic information" means electronic data and information, other than publicly available information and **[**information concerning**]**

a consumer's age or gender, that: (A) Concerns the business of a licensee and 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) concerns a consumer and that, because such data or information contains a name, number, personal mark or other identifier, can be used to identify such consumer in combination with: (i) A Social Security number; (ii) a driver's license number or nondriver identification card number; (iii) an account, credit or debit card number; (iv) an access or security code, or a password, that would permit access to the consumer's financial account; or (v) a biometric record; or (C) is in a form or medium created by, or derived from, a health care provider or consumer and concerns: (i) The past, present or future physical, mental or behavioral health or condition of a consumer or a member of a consumer's family; (ii) the provision of health care to a consumer; or (iii) payment for the provision of health care to a consumer.

(10) "Person" means any individual or any nongovernmental entity, including, but not limited to, any nongovernmental partnership, corporation, branch, agency or association.

(11) "Publicly available 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.

(12) "Risk assessment" means the risk assessment that each licensee is required to conduct pursuant to subdivision (3) of subsection (c) of this section.

(13) "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 otherwise permitted to access nonpublic information through the person's provision of services to a licensee.

(c) Information Security Program. (1) Implementation of an information security program. Except as provided in subdivision (10) of this subsection, each licensee shall, not later than October 1, **[**2020**]** 2021, develop, implement and maintain a comprehensive written information security program that is based on the licensee's risk assessment and contains the administrative, technical and physical safeguards for the protection of nonpublic information and such licensee's information systems. Each information security program shall be commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including, but not limited to, such licensee's use of third-party service providers, and the sensitivity of the nonpublic information used by such licensee or in such licensee's possession, custody or control.

(2) Objectives of Information Security Program. Except as provided in subdivision (10) of this subsection, each information security program developed, implemented and maintained by a licensee pursuant to subdivision (1) of this subsection shall:

(A) Be designed to:

(i) Protect the security and confidentiality of the nonpublic information and the security of the information system;

(ii) Protect against all threats and hazards to the security or integrity of nonpublic information and the information system; and

(iii) Protect against unauthorized access to, or use of, nonpublic information and minimize the likelihood of harm to any consumer; and

(B) Define, and periodically reevaluate, a schedule for retention of nonpublic information and a mechanism for the destruction of such information when such information no longer is needed.

(3) Risk Assessment. Except as provided in subdivision (10) of this subsection, each licensee shall:

(A) Designate one or more employees, an affiliate or an outside vendor designated to act on behalf of such licensee as the person responsible for such licensee's information security program;

(B) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of nonpublic information, including, but not limited to, the security of information systems that are, and nonpublic information that is, accessible to, or held by, third-party service providers;

(C) Assess the likelihood and potential damage of the threats identified pursuant to subparagraph (B) of this subdivision, taking into consideration the sensitivity of the nonpublic information;

(D) Assess the sufficiency of policies, procedures, information systems and other safeguards in place to manage the threats identified pursuant to subparagraph (B) of this subdivision by considering such threats in the following areas of such licensee's operations:

(i) Employee training and management;

(ii) Information systems, including, but not limited to, network and software design, as well as information classification, governance, processing, storage, transmission and disposal; and

(iii) Detection, prevention and response to attacks, intrusions or other systems failures;

(E) Implement information safeguards to manage the threats identified in such licensee's ongoing assessment; and

(F) Not less than annually, assess the effectiveness of such licensee's safeguards' key controls, systems and procedures.

(4) Risk Management. Except as provided in subdivision (10) of this subsection, each licensee shall, based on such licensee's risk assessment:

(A) Design such licensee's information security program to mitigate the identified risks, commensurate with the size and complexity of such licensee's activities, including, but not limited to, such licensee's use of third-party service providers, and the sensitivity of the nonpublic information used by such licensee or in such licensee's possession, custody or control.

(B) Determine which of the following security measures are appropriate and, if such measures are appropriate, implement such measures:

(i) Placement of access controls on such licensee's information systems, including, but not limited to, controls to authenticate and restrict access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information;

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

(iii) Restriction of access to physical locations containing nonpublic information only to authorized individuals;

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

(v) Adoption of secure development practices for in-house developed applications utilized by such licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by such licensee;

(vi) Modification of such licensee's information system in accordance

with such licensee's information security program;

(vii) Utilization of effective controls, which may include multifactor authentication procedures for any individual accessing nonpublic information;

(viii) Regular testing and monitoring of systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(ix) Inclusion of audit trails within the information security program that are designed to detect and respond to cybersecurity events, and designed to reconstruct material financial transactions sufficient to support the normal operations and obligations of the licensee;

(x) Implementation of measures to protect against the destruction, loss or damage of nonpublic information due to environmental hazards, including, but not limited to, fire and water, or other catastrophes or technological failures; and

(xi) Development, implementation and maintenance of procedures for the secure disposal of nonpublic information in any format.

(C) Include cybersecurity risks in such licensee's enterprise risk management process.

(D) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

(E) Provide such licensee's personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by such licensee in such licensee's risk assessment.

(5) Oversight by Board of Directors. Except as provided in subdivision (10) of this subsection, if a licensee has a board of directors, the board, or an appropriate committee of such board, shall, at a minimum:

(A) Require the licensee's executive management or **[**its**]** such executive management's delegates to develop, implement and maintain such licensee's information security program.

(B) Require the licensee's executive management or **[**its**]** such executive management's delegates to report, in writing and at least annually, the following information:

(i) The overall status of such licensee's information security program and such licensee's compliance with this section; and

(ii) Material matters related to such licensee's information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in such information security program.

(C) If a licensee's executive management delegates any of **[**its**]** such executive management's responsibilities under subparagraph (A) or (B) of this subdivision, **[**it**]** such executive management shall oversee the development, implementation and maintenance of the licensee's information security program prepared by the delegate or delegates, and shall receive a report from such delegate or delegates that satisfies the requirements established in subparagraph (B) of this subdivision.

(6) Oversight of Third-Party Service Provider Arrangements. Except as provided in subdivision (10) of this subsection:

(A) Each licensee shall exercise due diligence in selecting such licensee's third-party service providers; and

(B) Not later than October 1, **[**2021**]** 2022, each licensee shall require each of such licensee's third-party service providers to implement appropriate administrative, technical and physical measures to protect and secure the information systems that are, and nonpublic information that is, accessible to, or held by, such licensee's third-party service

providers.

(7) Program Adjustments. Except as provided in subdivision (10) of this subsection, each licensee shall monitor, evaluate and adjust, as appropriate, such licensee's information security program consistent with any relevant changes in technology, the sensitivity of **[**such licensee's**]** the nonpublic information in such licensee's possession, custody or control, internal or external threats to such information and such licensee's own changing business arrangements, including, but not limited to, changes stemming from mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

(8) Incident Response Plan. (A) Except as provided in subdivision (10) of this subsection, each licensee shall, as part of such licensee's information security program, establish a written incident response plan that is designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity or availability of nonpublic information that is in such licensee's possession, custody or control, such licensee's information systems or the continuing functionality of any aspect of such licensee's business or operations.

(B) Each incident response plan shall address the following areas:

(i) The internal process for responding to a cybersecurity event;

(ii) The goals of such incident response plan;

(iii) The definition of clear roles, responsibilities and levels of decision-making authority;

(iv) External and internal communications;

(v) Information sharing;

(vi) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(vii) Documentation and reporting regarding cybersecurity events and related incident response activities; and

(viii) Evaluation and revision, as necessary, of such incident response plan following each cybersecurity event.

(9) Annual Certification to Commissioner of Domiciliary State. Except as provided in subdivision (10) of this subsection, each insurer, health care center or fraternal benefit society domiciled in this state shall submit to the Insurance Commissioner a written statement, not later than February fifteenth, annually, certifying that such insurer, health care center or fraternal benefit society is in compliance with the requirements set forth in this subsection. A domestic insurer, health care center or fraternal benefit society that is a member of an insurance holding company system, as defined in section 38a-129, may submit one statement to the Insurance Commissioner on behalf of other domestic insurers, health care centers or fraternal benefit societies that are members of the same insurance holding company system, not later than February fifteenth, annually, certifying that such domestic members of the insurance holding company system are in compliance with the requirements set forth in this subsection. Each insurer, health care center or fraternal benefit society shall, either directly or through an affiliate, maintain, for examination by the Insurance Department, all records, schedules and data supporting each statement that such insurer, health care center or fraternal benefit society, or a member of an insurance holding company system acting on behalf of such insurer, health care center or fraternal benefit society, submits to the commissioner for a period of five years. To the extent an insurer, health care center or fraternal benefit society has identified areas, systems or processes that require material improvement, updating or redesign, the insurer, health care center or fraternal benefit society shall, either directly or through an affiliate, document such identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the commissioner.

(10) Exceptions. (A) The following exceptions shall apply to this subsection:

(i) (I) During the period beginning on October 1, **[**2020**]** 2021, and ending on September 30, **[**2021**]** 2022, each licensee with fewer than twenty employees, which, for the purposes of this subclause, includes independent contractors having access to the nonpublic information used by such licensee or in such licensee's possession, custody or control, shall be exempt from this subsection; and

(II) On and after October 1, **[**2021**]** 2022, each licensee with fewer than ten employees, which, for the purposes of this subclause, includes independent contractors having access to the nonpublic information used by such licensee or in such licensee's possession, custody or control, shall be exempt from this subsection;

(ii) 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 has established and maintains an information security program pursuant to said act and the rules, regulations, procedures or guidelines established thereunder, shall be deemed to have satisfied the requirements of this subsection, provided such licensee is in compliance therewith and submits to the Insurance Commissioner not later than February fifteenth, annually, a written statement certifying such licensee's compliance therewith;

(iii) Each employee, agent, representative or designee of a licensee, who is also a licensee, shall be exempt from the provisions of this subsection and need not develop its own information security program to the extent that such employee, agent, representative or designee is covered by the other licensee's information security program; and

(iv) Each licensee that has established and maintains an information security program in compliance with **[**the statutes, rules and regulations of a jurisdiction approved by the commissioner pursuant to regulations adopted pursuant to subsection (i) of this section**]** Part 500 of Chapter I of Title 23 of the New York Codes, Rules and Regulations, as amended

from time to time, shall be deemed to have satisfied the provisions of this subsection, provided such licensee is in compliance therewith and submits to the commissioner, not later than February fifteenth, annually, a written statement certifying such licensee's compliance therewith.

(B) In the event that a licensee ceases to qualify for an exception under this subdivision, the licensee shall have one hundred eighty days to comply with this subsection.

(d) Investigation of a Cybersecurity Event. (1) If a licensee learns that a cybersecurity event has, or may have, occurred, the licensee, or an outside vendor or service provider, or both, designated to act on behalf of such licensee, shall conduct a prompt investigation in accordance with the provisions of this subsection.

(2) During any investigation conducted pursuant to subdivision (1) of this subsection, the licensee or the outside vendor or service provider, or both, shall, at a minimum and to the extent possible:

(A) Determine whether the cybersecurity event occurred; and

(B) If the cybersecurity event occurred:

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

(ii) Identify the nonpublic information, if any, that may have been involved in such cybersecurity event; and

(iii) Perform or oversee reasonable measures to restore the security of the information systems compromised in such cybersecurity event in order to prevent further unauthorized acquisition, release or use of nonpublic information that is in the licensee's possession, custody or control.

(3) If a licensee learns that a cybersecurity event has, or may have, occurred in a system maintained by a third-party service provider, the licensee shall complete the steps listed in subdivision (2) of this subsection or confirm and document that the third-party service

provider has completed such steps.

(4) Each licensee that is subject to the provisions of this subsection shall maintain records concerning each cybersecurity event for a period of at least five years from the date of such cybersecurity event, and shall produce such records to the Insurance Commissioner upon demand by the commissioner.

(e) Notification of a Cybersecurity Event. (1) Notification to the Commissioner. Each licensee shall notify the Insurance Commissioner that a cybersecurity event has occurred, as promptly as possible but in no event later than three business days after the date **[**of the**]** on which such licensee first determines that a cybersecurity event has occurred, if:

(A) Such licensee is an insurer and this state is the insurer's state of domicile, or the licensee is an insurance producer, as defined in section 38a-702a, and this state is the insurance producer's home state, as defined in section 38a-702a; **[**and**]** or

(B) The licensee reasonably believes that the nonpublic information involved in the cybersecurity event is of two hundred fifty or more consumers residing in this state and:

(i) State or federal law requires that a notice concerning such cybersecurity event be provided to a government body, self-regulatory agency or another supervisory body; or

(ii) It is reasonably likely that such cybersecurity event will materially harm:

(I) A consumer residing in this state; or

(II) A material part of such licensee's normal operations.

(2) Information to Be Provided to Commissioner. (A) Each licensee that notifies the Insurance Commissioner pursuant to subdivision (1) of this subsection shall provide to the commissioner, in an electronic form prescribed by the commissioner, as much of the following information

as possible:

(i) The date of the cybersecurity event;

(ii) A description of how the information was exposed, lost, stolen or breached, including, but not limited to, the specific roles and responsibilities of third-party service providers, if any;

(iii) How, and the date on which, the cybersecurity event was discovered;

(iv) Whether any lost, stolen or breached information has been recovered, and, if so, how such information was recovered;

(v) The identity of the source of the cybersecurity event;

(vi) Whether such licensee has filed a police report or notified any regulatory, government or law enforcement agency, and, if so, when such licensee filed such report or provided such notice;

(vii) A description of the specific types of exposed, lost, stolen or breached information, including, for example, specific types of medical information, financial information or information allowing identification of a consumer;

(viii) The period during which each information system that was compromised by the cybersecurity event was compromised by such cybersecurity event;

(ix) The number of total consumers residing in this state that, within such licensee's knowledge at the time that such licensee discloses such number to the commissioner, are affected by the cybersecurity event;

(x) The results of an internal review identifying any lapse in automated controls or internal procedures, or confirming that all such controls and procedures were followed;

(xi) A description of any efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur;

(xii) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event; and

(xiii) The name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

(B) Each licensee that provides information to the Insurance Commissioner pursuant to subparagraph (A) of this subdivision shall have a continuing obligation to update and supplement such information.

(3) Notification to Consumers. Each licensee shall comply with all applicable provisions of section 36a-701b, and provide to the Insurance Commissioner a copy of the notice that such licensee sends to consumers pursuant to said section, if any, if such licensee is required to notify the commissioner pursuant to subdivision (1) of this subsection.

(4) Notice Regarding Cybersecurity Events of Third-Party Service Providers. (A) In the case of a cybersecurity event involving **[**a**]** an information system maintained by a third-party service provider, each licensee affected by the event shall treat such event, if the licensee **[**as**]** is aware of such event, as such licensee would treat such event under subdivision (1) of this subsection.

(B) The computation of a licensee's deadlines shall begin on the day after a third-party service provider notifies the licensee of the cybersecurity event or such licensee otherwise first **[**becomes aware**]** has actual knowledge of such event, whichever is sooner.

(C) Nothing in this section shall prevent or abrogate an agreement between a licensee and another party to fulfill any of the investigation requirements imposed under subsection (d) of this section or the notice requirements imposed under this subsection.

(5) Notice Regarding Cybersecurity Events of Reinsurers to Insurers.

(A) (i) In the case of a cybersecurity event involving nonpublic information that is used by a licensee that is acting as an assuming insurer or in the possession, custody or control of a licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify its affected ceding insurers and the insurance regulatory official of its state of domicile not later than seventy-two hours after such assuming insurer discovered that the cybersecurity event had occurred.

(ii) Each ceding insurer that has a direct contractual relationship with the consumers affected by a cybersecurity event shall fulfill the consumer notification requirements imposed under section 36a-701b and any other notification requirements relating to a cybersecurity event imposed under this section.

(B) (i) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a third-party service provider of a licensee, when the licensee is acting as an assuming insurer, including an assuming insurer that is domiciled in another state or jurisdiction, the assuming insurer shall notify its affected ceding insurers and the insurance regulatory official of its state of domicile not later than seventy-two hours after such assuming insurer received notice from the third-party service provider disclosing that the cybersecurity event occurred.

(ii) Ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under section 36a-701b and any other notification requirements relating to a cybersecurity event imposed under this section.

(6) Notice Regarding Cybersecurity Events of Insurers to Producers of Record. If a cybersecurity event involves nonpublic information that is in the possession, custody or control of a licensee that is an insurer, or a third-party service provider for a licensee that is an insurer, and for which a consumer who is affected by the cybersecurity event accessed

such licensee's services through an independent insurance producer, such licensee shall notify the producer of record for such consumer of the occurrence of such cybersecurity event in a reasonable manner and not later than the time at which notice is provided to such consumer, provided such licensee has the current producer of record information for such individual consumer.

(f) Power of Commissioner. (1) The Insurance Commissioner shall have power to examine and investigate into the affairs of a licensee to determine whether the licensee is, or has been, engaged in conduct in this state that violates the provisions of this section. The commissioner's power under this subsection is in addition to the commissioner's powers under sections 38a-14 to 38a-16, inclusive. Any such investigation or examination shall be conducted pursuant to said sections, if applicable.

(2) Whenever the Insurance Commissioner has reason to believe that a licensee is, or has been, engaged in conduct in this state that violates the provisions of this section, the commissioner shall issue and serve upon the licensee:

(A) A statement setting forth such violation; and

(B) A 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.

(3) (A) The licensee shall, at the time and place fixed for the hearing in the notice issued and served upon such licensee pursuant to subdivision (2) of this subsection, have an opportunity to be heard and show cause why an order should not be entered by the Insurance 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 Insurance Commissioner has issued, or may issue, to such licensee.

(B) The Insurance 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 the licensee, impose on such licensee a civil penalty of not more than fifty thousand dollars for each violation of the provisions of this section. The commissioner may bring a civil action to recover the amount of any civil penalty that the commissioner imposes on a licensee pursuant to this subparagraph.

(g) Confidentiality. (1) (A) Except as provided in subparagraph (B) of this subdivision, documents, materials and other information in the possession, custody or control of the Insurance Department and furnished to the department by a licensee, or an employee or agent of a licensee acting on behalf of the licensee, pursuant to subdivision (9) of subsection (c) of this section or subparagraph (A)(ii), (A)(iii), (A)(iv), (A)(v), (A)(viii), (A)(x) or (A)(xi) of subdivision (2) of subsection (e) of this section, or obtained by the commissioner in an investigation or examination conducted pursuant to subsection (f) of this section, shall be confidential by law, privileged, not subject to disclosure under section 1-210, not subject to subpoena, and not subject to discovery or admission into evidence in any private civil action.

(B) The Insurance Commissioner is authorized to use all documents, materials and other information in furtherance of any regulatory or legal actions brought as a part of the commissioner's duties.

(2) Neither the Insurance Commissioner nor any person acting under the authority of the commissioner who receives documents or materials that are, or other information that is, subject to the provisions of subdivision (1) of this subsection shall be permitted or required to testify in any private civil action concerning such documents, materials or other information.

(3) The Insurance Commissioner, in **[**order to assist the commissioner in performing**]** furtherance of the commissioner's duties under this

section, may:

(A) Share documents, materials and other information, including, but not limited to, confidential and privileged documents, materials and other information subject to subdivision (1) of this subsection, with other state, federal and international regulatory agencies, the National Association of Insurance Commissioners and the affiliates and subsidiaries of said association, the Attorney General and other state, federal or international law enforcement authorities, provided the recipient of such documents, materials or other information agrees, in writing, to maintain the confidentiality and privileged status of such documents, materials or other information;

(B) Receive documents, materials and other information, including, but not limited to, otherwise confidential and privileged documents, materials and other information, from the National Association of Insurance Commissioners and the affiliates and subsidiaries of said association, the Attorney General and other domestic or foreign regulatory or law enforcement officials, provided the commissioner shall maintain as confidential and privileged all documents, materials and other information that the commissioner receives with notice or an understanding that such documents or materials are, or such other information is, confidential or privileged under the laws of the jurisdiction that is the source of such documents, materials or other information;

(C) Share documents, materials and other information subject to subdivision (1) of this subsection with a third-party consultant or vendor, provided the third-party consultant or vendor agrees, in writing, to maintain the confidentiality and privileged status of such documents, materials and other information; and

(D) Enter into agreements governing the sharing and use of documents, materials and other information, provided such agreements are consistent with the provisions of this subsection.

(4) No waiver of any applicable privilege or claim of confidentiality

in a document, material or other information shall occur as a result of any disclosure of the document, material or other information to the Insurance Commissioner pursuant to this section, or as a result of any sharing of such document, material or other information authorized under subdivision (3) of this subsection.

(5) Nothing in this section shall prohibit the Insurance Commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to section 1-210 to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners or the affiliates or subsidiaries of said association.

(6) All documents, materials and other information provided to, and in the possession, custody or control of, the National Association of Insurance Commissioners or a third-party consultant or vendor pursuant to this section shall be confidential by law, privileged, not be subject to disclosure under section 1-210, not subject to subpoena, and not subject to discovery or admission into evidence in any private civil action.

Sec. 4. Subsection (g) of section 38a-48 of the 2020 supplement to the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2020*):

(g) If the actual expenditures for the fall prevention program established in section 17a-303a are less than the amount allocated, the Commissioner of Aging and Disability Services shall notify the Insurance Commissioner and the Healthcare Advocate. Immediately following the close of the fiscal year, the Insurance Commissioner and the Healthcare Advocate shall recalculate the proposed assessment for each domestic insurance company or other domestic entity in accordance with subsection (c) of this section using the actual expenditures made during the fiscal year by the Insurance Department, the Office of the Healthcare Advocate and the Office of Health Strategy from the Insurance Fund, the actual expenditures made on behalf of the department and the offices from the Capital Equipment Purchase Fund

pursuant to section 4a-9, not including such expenditures made on behalf of the Health Systems Planning Unit of the Office of Health Strategy, and the actual expenditures for the fall prevention program. On or before July thirty-first, the Insurance Commissioner and the Healthcare Advocate shall render to each such domestic insurance company and other domestic entity a statement showing the difference between their respective recalculated assessments and the amount they have previously paid. On or before August thirty-first, the Insurance Commissioner and the Healthcare Advocate, after receiving any objections to such statements, shall make such adjustments which in their opinion may be indicated, and shall render an adjusted assessment, if any, to the affected companies. Any such domestic insurance company or other domestic entity may pay to the Insurance Commissioner the entire assessment required under this subsection in one payment when the first installment of such assessment is due.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*July 1, 2020*	19a-7p(b) and (c)
Sec. 2	*October 1, 2020*	38a-8(d)
Sec. 3	*October 1, 2020*	38a-38(b) to (g)
Sec. 4	*July 1, 2020*	38a-48(g)

Statement of Purpose:

To (1) modify reporting requirements, and impose a late filing fee and penalty, concerning the public health fee, (2) permit attorneys, actuaries, accountants and experts to perform certain duties currently performed by the Insurance Department's employees, (3) modify the Insurance Data Security Law, and (4) modify the payment schedule for assessments against domestic insurance companies and other domestic entities.

[Proposed deletions are enclosed in brackets. Proposed additions are indicated by underline, except that when the entire text of a bill or resolution or a section of a bill or resolution is new, it is not underlined.]