

**Proposed Substitute  
Bill No. 5365**

LCO No. 2961

**AN ACT CONCERNING THE INSURANCE DEPARTMENT'S  
RECOMMENDATIONS REGARDING THE PUBLIC HEALTH FEE, 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:

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2 supplement to the general statutes are repealed and the following is  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

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

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

13 (3) (A) Not later than September first, annually, each such insurer or  
14 health care center shall report to the Insurance Commissioner, in the  
15 form and manner prescribed by [said] the commissioner, the number of  
16 insured or enrolled lives in this state as of May first immediately  
17 preceding the date for which such insurer or health care center is

18 providing health insurance that provides coverage of the types specified  
19 in subdivisions (1), (2), (4), (11) and (12) of section 38a-469. Such number  
20 shall not include lives enrolled in Medicare, any medical assistance  
21 program administered by the Department of Social Services, workers'  
22 compensation insurance or Medicare Part C plans. The commissioner  
23 may require each such insurer or health care center or any other person  
24 to submit to the commissioner any records that are in such insurer's,  
25 health care center's or other person's possession if such records were  
26 used to prepare such insurer's or health care center's annual report  
27 submitted pursuant to this subparagraph.

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

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

41 (c) Not later than November first, annually, the Insurance  
42 Commissioner shall determine the fee to be assessed for the current  
43 fiscal year against each such insurer and health care center. Such fee  
44 shall be calculated by multiplying the number of lives reported to said  
45 commissioner pursuant to subparagraph (A) of subdivision (3) of  
46 subsection (b) of this section by a factor, determined annually by said  
47 commissioner as set forth in this subsection, to fully fund the aggregate  
48 amount determined under subsection (a) of this section. The Insurance  
49 Commissioner shall determine the factor by dividing the aggregate

50 amount by the total number of lives reported to said commissioner  
51 pursuant to subparagraph (A) of subdivision (3) of subsection (b) of this  
52 section.

53 Sec. 2. Subsections (b) to (g), inclusive, of section 38a-38 of the 2020  
54 supplement to the general statutes are repealed and the following is  
55 substituted in lieu thereof (*Effective October 1, 2020*):

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

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

61 (2) "Consumer" means an individual, including, but not limited to, an  
62 applicant, beneficiary, certificate holder, claimant, insured or  
63 policyholder, who is a resident of this state and whose nonpublic  
64 information is in a licensee's possession, custody or control.

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

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

78 (5) "Information security program" means the administrative,  
79 technical and physical safeguards that a licensee uses to access, collect,

80 distribute, process, protect, store, use, transmit, dispose of or otherwise  
81 handle nonpublic information.

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

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

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

105 (9) "Nonpublic information" means electronic data and information,  
106 other than publicly available information and [information concerning]  
107 a consumer's age or gender, that: (A) Concerns the business of a licensee  
108 and that, if accessed, disclosed, tampered with or used without  
109 authorization from the licensee, would have a material adverse impact  
110 on the business, operations or security of such licensee; (B) concerns a  
111 consumer and that, because such data or information contains a name,

112 number, personal mark or other identifier, can be used to identify such  
113 consumer in combination with: (i) A Social Security number; (ii) a  
114 driver's license number or nondriver identification card number; (iii) an  
115 account, credit or debit card number; (iv) an access or security code, or  
116 a password, that would permit access to the consumer's financial  
117 account; or (v) a biometric record; or (C) is in a form or medium created  
118 by, or derived from, a health care provider or consumer and concerns:  
119 (i) The past, present or future physical, mental or behavioral health or  
120 condition of a consumer or a member of a consumer's family; (ii) the  
121 provision of health care to a consumer; or (iii) payment for the provision  
122 of health care to a consumer.

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

126 (11) "Publicly available information" means data or information that:  
127 (A) (i) Must be disclosed to the general public pursuant to applicable  
128 law; or (ii) may be made available to the general public from  
129 government records or widely distributed media; and (B) a licensee  
130 reasonably believes, after investigation: (i) Is of a type that is available  
131 to the general public; and (ii) the consumer has not directed to be  
132 withheld from the general public, if the consumer may direct that such  
133 data or information be withheld from the general public pursuant to  
134 applicable law.

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

138 (13) "Third-party service provider" means a person, other than a  
139 licensee, that: (A) Contracts with a licensee to maintain, process or store  
140 nonpublic information; or (B) is otherwise permitted to access nonpublic  
141 information through the person's provision of services to a licensee.

142 (c) Information Security Program. (1) Implementation of an

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

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

159 (A) Be designed to:

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

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

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

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

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

171 (A) Designate one or more employees, an affiliate or an outside

172 vendor designated to act on behalf of such licensee as the person  
173 responsible for such licensee's information security program;

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

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

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

187 (i) Employee training and management;

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

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

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

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

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

199 (A) Design such licensee's information security program to mitigate

200 the identified risks, commensurate with the size and complexity of such  
201 licensee's activities, including, but not limited to, such licensee's use of  
202 third-party service providers, and the sensitivity of the nonpublic  
203 information used by such licensee or in such licensee's possession,  
204 custody or control.

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

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

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

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

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

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

226 (vi) Modification of such licensee's information system in accordance  
227 with such licensee's information security program;

228 (vii) Utilization of effective controls, which may include multifactor

229 authentication procedures for any individual accessing nonpublic  
230 information;

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

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

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

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

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

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

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

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

256 (A) Require the licensee's executive management or [its] such

257 executive management's delegates to develop, implement and maintain  
258 such licensee's information security program.

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

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

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

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

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

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

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

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

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

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

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

308 (ii) The goals of such incident response plan;

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

311 (iv) External and internal communications;

312 (v) Information sharing;

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

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

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

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

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

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

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

361 (ii) Each licensee that is subject to the Health Insurance Portability  
362 and Accountability Act of 1996, P.L. 104-191, as amended from time to  
363 time, and has established and maintains an information security  
364 program pursuant to said act and the rules, regulations, procedures or  
365 guidelines established thereunder, shall be deemed to have satisfied the  
366 requirements of this subsection, provided such licensee is in compliance  
367 therewith and submits to the Insurance Commissioner not later than  
368 February fifteenth, annually, a written statement certifying such  
369 licensee's compliance therewith;

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

375 (iv) Each licensee that has established and maintains an information  
376 security program in compliance with [the statutes, rules and regulations  
377 of a jurisdiction approved by the commissioner pursuant to regulations  
378 adopted pursuant to subsection (i) of this section] Part 500 of Chapter I

379 of Title 23 of the New York Codes, Rules and Regulations, as amended  
380 from time to time, shall be deemed to have satisfied the provisions of  
381 this subsection, provided such licensee is in compliance therewith and  
382 submits to the commissioner, not later than February fifteenth, annually,  
383 a written statement certifying such licensee's compliance therewith.

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

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

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

395 (A) Determine whether the cybersecurity event occurred; and

396 (B) If the cybersecurity event occurred:

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

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

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

405 (3) If a licensee learns that a cybersecurity event has, or may have,  
406 occurred in a system maintained by a third-party service provider, the

407 licensee shall complete the steps listed in subdivision (2) of this  
408 subsection or confirm and document that the third-party service  
409 provider has completed such steps.

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

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

420 (A) Such licensee is an insurer and this state is the insurer's state of  
421 domicile, or the licensee is an insurance producer, as defined in section  
422 38a-702a, and this state is the insurance producer's home state, as  
423 defined in section 38a-702a; [and] or

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

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

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

432 (I) A consumer residing in this state; or

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

434 (2) Information to Be Provided to Commissioner. (A) Each licensee

435 that notifies the Insurance Commissioner pursuant to subdivision (1) of  
436 this subsection shall provide to the commissioner, in an electronic form  
437 prescribed by the commissioner, as much of the following information  
438 as possible:

439 (i) The date of the cybersecurity event;

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

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

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

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

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

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

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

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

461 (x) The results of an internal review identifying any lapse in  
462 automated controls or internal procedures, or confirming that all such

463 controls and procedures were followed;

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

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

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

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

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

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

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

491 (C) Nothing in this section shall prevent or abrogate an agreement

492 between a licensee and another party to fulfill any of the investigation  
493 requirements imposed under subsection (d) of this section or the notice  
494 requirements imposed under this subsection.

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

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

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

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

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

523 (6) Notice Regarding Cybersecurity Events of Insurers to Producers  
524 of Record. If a cybersecurity event involves nonpublic information that  
525 is in the possession, custody or control of a licensee that is an insurer, or  
526 a third-party service provider for a licensee that is an insurer, and for  
527 which a consumer who is affected by the cybersecurity event accessed  
528 such licensee's services through an independent insurance producer,  
529 such licensee shall notify the producer of record for such consumer of  
530 the occurrence of such cybersecurity event in a reasonable manner and  
531 not later than the time at which notice is provided to such consumer,  
532 provided such licensee has the current producer of record information  
533 for such individual consumer.

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

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

545 (A) A statement setting forth such violation; and

546 (B) A notice of a hearing to be held at a time and place fixed in such  
547 notice, which time shall not be less than thirty calendar days after the  
548 date of service of such notice.

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

554 (i) Enforcing the provisions of this section; or

555 (ii) Suspending, revoking or refusing to reissue or renew any license,  
556 certificate of registration or authorization to operate the Insurance  
557 Commissioner has issued, or may issue, to such licensee.

558 (B) The Insurance Commissioner may, after holding a hearing  
559 pursuant to subparagraph (A) of this subdivision and in addition to or  
560 in lieu of suspending, revoking or refusing to reissue or renew any  
561 license, certificate of registration or authorization to operate the  
562 commissioner has issued, or may issue, to the licensee, impose on such  
563 licensee a civil penalty of not more than fifty thousand dollars for each  
564 violation of the provisions of this section. The commissioner may bring  
565 a civil action to recover the amount of any civil penalty that the  
566 commissioner imposes on a licensee pursuant to this subparagraph.

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

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

582 (2) Neither the Insurance Commissioner nor any person acting under  
583 the authority of the commissioner who receives documents or materials  
584 that are, or other information that is, subject to the provisions of

585 subdivision (1) of this subsection shall be permitted or required to testify  
586 in any private civil action concerning such documents, materials or  
587 other information.

588 (3) The Insurance Commissioner, in [order to assist the commissioner  
589 in performing] furtherance of the commissioner's duties under this  
590 section, may:

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

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

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

617 documents, materials and other information; and

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

621 (4) No waiver of any applicable privilege or claim of confidentiality  
622 in a document, material or other information shall occur as a result of  
623 any disclosure of the document, material or other information to the  
624 Insurance Commissioner pursuant to this section, or as a result of any  
625 sharing of such document, material or other information authorized  
626 under subdivision (3) of this subsection.

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

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

639 Sec. 3. Subsection (g) of section 38a-48 of the 2020 supplement to the  
640 general statutes is repealed and the following is substituted in lieu  
641 thereof (*Effective July 1, 2020*):

642 (g) If the actual expenditures for the fall prevention program  
643 established in section 17a-303a are less than the amount allocated, the  
644 Commissioner of Aging and Disability Services shall notify the  
645 Insurance Commissioner and the Healthcare Advocate. Immediately  
646 following the close of the fiscal year, the Insurance Commissioner and

647 the Healthcare Advocate shall recalculate the proposed assessment for  
648 each domestic insurance company or other domestic entity in  
649 accordance with subsection (c) of this section using the actual  
650 expenditures made during the fiscal year by the Insurance Department,  
651 the Office of the Healthcare Advocate and the Office of Health Strategy  
652 from the Insurance Fund, the actual expenditures made on behalf of the  
653 department and the offices from the Capital Equipment Purchase Fund  
654 pursuant to section 4a-9, not including such expenditures made on  
655 behalf of the Health Systems Planning Unit of the Office of Health  
656 Strategy, and the actual expenditures for the fall prevention program.  
657 On or before July thirty-first, the Insurance Commissioner and the  
658 Healthcare Advocate shall render to each such domestic insurance  
659 company and other domestic entity a statement showing the difference  
660 between their respective recalculated assessments and the amount they  
661 have previously paid. On or before August thirty-first, the Insurance  
662 Commissioner and the Healthcare Advocate, after receiving any  
663 objections to such statements, shall make such adjustments which in  
664 their opinion may be indicated, and shall render an adjusted  
665 assessment, if any, to the affected companies. Any such domestic  
666 insurance company or other domestic entity may pay to the Insurance  
667 Commissioner the entire assessment required under this subsection in  
668 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	<i>July 1, 2020</i>	19a-7p(b) and (c)
Sec. 2	<i>October 1, 2020</i>	38a-38(b) to (g)
Sec. 3	<i>July 1, 2020</i>	38a-48(g)