

House Amendments to Senate Bill No. 2831

TO THE SECRETARY OF THE SENATE:

THIS IS TO INFORM YOU THAT THE HOUSE HAS ADOPTED THE AMENDMENTS SET OUT BELOW:

AMENDMENT NO. 1

Amend by striking all after the enacting clause and inserting in lieu thereof the following:

12 SECTION 1. This act shall be known and may be cited as the
13 "Insurance Data Security Law."

14 SECTION 2. (1) Notwithstanding any other provision of law,
15 this act establishes the exclusive state standards applicable to
16 licensees for data security, the investigation of a cybersecurity
17 event as defined in Section 3 of this act, and notification to the
18 Commissioner of Insurance.

19 (2) This act may not be construed to create or imply a
20 private cause of action for violation of its provisions nor may it
21 be construed to curtail a private cause of action which would
22 otherwise exist in the absence of this act.

23 SECTION 3. As used in this act, the following terms shall
24 have the following meanings:

25 (a) "Authorized individual" means an individual known
26 to and screened by the licensee and determined to be necessary and
27 appropriate to have access to the nonpublic information held by
28 the licensee and its information systems.

29 (b) "Commissioner" means the Commissioner of Insurance.

30 (c) "Consumer" means an individual, including, but not
31 limited to, applicants, policyholders, insureds, beneficiaries,
32 claimants and certificate holders, who is a resident of this state
33 and whose nonpublic information is in a licensee's possession,
34 custody or control.

35 (d) "Cybersecurity event" means an event resulting in
36 unauthorized access to, disruption or misuse of, an information
37 system or nonpublic information stored on such information system.
38 The term "cybersecurity event" does not include the unauthorized
39 acquisition of encrypted nonpublic information if the encryption,
40 process or key is not also acquired, released or used without
41 authorization. "Cybersecurity event" does not include an event
42 with regard to which the licensee has determined that the
43 nonpublic information accessed by an unauthorized person has not
44 been used or released and has been returned or destroyed.

45 (e) "Department" means the Mississippi Insurance
46 Department.

47 (f) "Encrypted" means the transformation of data into a
48 form which results in a low probability of assigning meaning
49 without the use of a protective process or key.

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

54 (h) "Information system" means a discrete set of
55 electronic information resources organized for the collection,
56 processing, maintenance, use, sharing, dissemination or
57 disposition of electronic nonpublic information, as well as any
58 specialized system such as industrial/process controls systems,
59 telephone switching and private branch exchange systems, and
60 environmental control systems.

61 (i) "Licensee" means any person licensed, authorized to
62 operate, or registered, or required to be licensed, authorized, or
63 registered pursuant to the insurance laws of this state but shall
64 not include a purchasing group or a risk-retention group chartered
65 and licensed in a state other than this state or a person that is
66 acting as an assuming insurer that is domiciled in another state
67 or jurisdiction.

68 (j) "Multi-factor authentication" means authentication
69 through verification of at least two (2) of the following types of
70 authentication factors:

71 (i) Knowledge factors, such as a password;

72 (ii) Possession factors, such as a token or text
73 message on a mobile phone; or

74 (iii) Inherence factors, such as a biometric
75 characteristic.

76 (k) "Nonpublic information" means electronic
77 information that is not publicly available information and is:

78 (i) Any information concerning a consumer which
79 because of name, number, personal mark or other identifier can be

80 used to identify such consumer, in combination with any one or
81 more of the following data elements:

82 1. Social security number;

83 2. Driver's license number or nondriver
84 identification card number;

85 3. Financial account number, credit or debit
86 card number;

87 4. Any security code, access code or password
88 that would permit access to a consumer's financial account; or

89 5. Biometric records;

90 (ii) Any information or data, except age or
91 gender, in any form or medium created by or derived from a health
92 care provider or a consumer, that can be used to identify a
93 particular consumer, and that relates to:

94 1. The past, present or future physical,
95 mental or behavioral health or condition of any consumer or a
96 member of the consumer's family;

97 2. The provision of health care to any
98 consumer; or

99 3. Payment for the provision of health care
100 to any consumer.

101 (1) "Person" means any individual or any
102 nongovernmental entity, including, but not limited to, any
103 nongovernmental partnership, corporation, branch, agency or
104 association.

105 (m) "Publicly available information" means any
106 information that a licensee has a reasonable basis to believe is
107 lawfully made available to the general public from: federal,
108 state or local government records; widely distributed media; or
109 disclosures to the general public that are required to be made by
110 federal, state or local law. For the purposes of this definition,
111 a licensee has a reasonable basis to believe that information is
112 lawfully made available to the general public if the licensee has
113 taken steps to determine:

114 (i) That the information is of the type that is
115 available to the general public; and

116 (ii) Whether a consumer can direct that the
117 information not be made available to the general public and, if
118 so, that such consumer has not done so.

119 (n) "Risk assessment" means the risk assessment that
120 each licensee is required to conduct under Section 4(3) of this
121 act.

122 (o) "State" means the State of Mississippi.

123 (p) "Third-party service provider" means a person, not
124 otherwise defined as a licensee, that contracts with a licensee to
125 maintain, process, store or otherwise is permitted access to
126 nonpublic information through its provision of services to the
127 licensee.

128 **SECTION 4.** (1) Commensurate with the size and complexity of
129 the licensee, the nature and scope of the licensee's activities,
130 including its use of third-party service providers, and the

131 sensitivity of the nonpublic information used by the licensee or
132 in the licensee's possession, custody or control, each licensee
133 shall develop, implement, and maintain a comprehensive written
134 information security program based on the licensee's risk
135 assessment and that contains administrative, technical and
136 physical safeguards for the protection of nonpublic information
137 and the licensee's information system.

138 (2) A licensee's information security program shall be
139 designed to:

140 (a) Protect the security and confidentiality of
141 nonpublic information and the security of the information system;

142 (b) Protect against any threats or hazards to the
143 security or integrity of nonpublic information and the information
144 system;

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

148 (d) Define and periodically reevaluate a schedule for
149 retention of nonpublic information and a mechanism for its
150 destruction when no longer needed.

151 (3) The licensee shall:

152 (a) Designate one or more employees, an affiliate, or
153 an outside vendor designated to act on behalf of the licensee who
154 is responsible for the information security program;

155 (b) Identify reasonably foreseeable internal or
156 external threats that could result in unauthorized access,

157 transmission, disclosure, misuse, alteration or destruction of
158 nonpublic information, including the security of information
159 systems and nonpublic information that are accessible to, or held
160 by, third-party service providers;

161 (c) Assess the likelihood and potential damage of these
162 threats, taking into consideration the sensitivity of the
163 nonpublic information;

164 (d) Assess the sufficiency of policies, procedures,
165 information systems and other safeguards in place to manage these
166 threats, including consideration of threats in each relevant area
167 of the licensee's operations, including:

168 (i) Employee training and management;

169 (ii) Information systems, including network and
170 software design, as well as information classification,
171 governance, processing, storage, transmission and disposal; and

172 (iii) Detecting, preventing and responding to
173 attacks, intrusions or other systems failures; and

174 (e) Implement information safeguards to manage the
175 threats identified in its ongoing assessment, and no less than
176 annually, assess the effectiveness of the safeguards' key
177 controls, systems and procedures.

178 (4) Based on its risk assessment, the licensee shall:

179 (a) Design its information security program to mitigate
180 the identified risks, commensurate with the size and complexity of
181 the licensee, the nature and scope of the licensee's activities,
182 including its use of third-party service providers, and the

183 sensitivity of the nonpublic information used by the licensee or
184 in the licensee's possession, custody or control.

185 (b) Determine which security measures listed below are
186 appropriate and implement such security measures.

187 (i) Place access controls on information systems,
188 including controls to authenticate and permit access only to
189 authorized individuals to protect against the unauthorized
190 acquisition of nonpublic information;

191 (ii) Identify and manage the data, personnel,
192 devices, systems and facilities that enable the organization to
193 achieve business purposes in accordance with their relative
194 importance to business objectives and the organization's risk
195 strategy;

196 (iii) Restrict physical access to nonpublic
197 information, only to authorized individuals;

198 (iv) Protect by encryption or other appropriate
199 means, all nonpublic information while being transmitted over an
200 external network and all nonpublic information stored on a laptop
201 computer or other portable computing or storage device or media;

202 (v) Adopt secure development practices for
203 in-house developed applications utilized by the licensee;

204 (vi) Modify the information system in accordance
205 with the licensee's information security program;

206 (vii) Utilize effective controls, which may
207 include multi-factor authentication procedures for employees
208 accessing nonpublic information;

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

212 (ix) Include audit trails within the information
213 security program designed to detect and respond to cybersecurity
214 events and designed to reconstruct material financial transactions
215 sufficient to support normal operations and obligations of the
216 licensee;

217 (x) Implement measures to protect against
218 destruction, loss, or damage of nonpublic information due to
219 environmental hazards, such as fire and water damage or other
220 catastrophes or technological failures; and

221 (xi) Develop, implement, and maintain procedures
222 for the secure disposal of nonpublic information in any format.

223 (c) Include cybersecurity risks in the licensee's
224 enterprise risk management process.

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

229 (e) Provide its personnel with cybersecurity awareness
230 training that is updated as necessary to reflect risks identified
231 by the licensee in the risk assessment.

232 (5) If the licensee has a board of directors, the board or
233 an appropriate committee of the board shall, at a minimum:

234 (a) Require the licensee's executive management or its
235 delegates to develop, implement and maintain the licensee's
236 information security program;

237 (b) Require the licensee's executive management or its
238 delegates to report in writing at least annually, the following
239 information:

240 (i) The overall status of the information security
241 program and the licensee's compliance with this act; and

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

248 (c) If executive management delegates any of its
249 responsibilities under this section, it shall oversee the
250 development, implementation and maintenance of the licensee's
251 information security program prepared by the delegate(s) and shall
252 receive a report from the delegate(s) complying with the
253 requirements of the report to the board of directors above.

254 (6) (a) A licensee shall exercise due diligence in
255 selecting its third-party service provider; and

256 (b) A licensee shall require a third-party service
257 provider to implement appropriate administrative, technical and
258 physical measures to protect and secure the information systems

259 and nonpublic information that are accessible to, or held by, the
260 third-party service provider.

261 (7) The licensee shall monitor, evaluate and adjust, as
262 appropriate, the information security program consistent with any
263 relevant changes in technology, the sensitivity of its nonpublic
264 information, internal or external threats to information, and the
265 licensee's own changing business arrangements, such as mergers and
266 acquisitions, alliances and joint ventures, outsourcing
267 arrangements and changes to information systems.

268 (8) (a) As part of its information security program, each
269 licensee shall establish a written incident response plan designed
270 to promptly respond to, and recover from, any cybersecurity event
271 that compromises the confidentiality, integrity or availability of
272 nonpublic information in its possession, the licensee's
273 information systems, or the continuing functionality of any aspect
274 of the licensee's business or operations.

275 (b) Such incident response plan shall address the
276 following areas:

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

279 (ii) The goals of the incident response plan;

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

282 (iv) External and internal communications and
283 information sharing;

284 (v) Identification of requirements for the
285 remediation of any identified weaknesses in information systems
286 and associated controls;

287 (vi) Documentation and reporting regarding
288 cybersecurity events and related incident response activities; and

289 (vii) The evaluation and revision as necessary of
290 the incident response plan following a cybersecurity event.

291 (9) Annually, each insurer domiciled in this state shall
292 submit to the commissioner, a written statement by February 15,
293 certifying that the insurer is in compliance with the requirements
294 set forth in this section. Each insurer shall maintain for
295 examination by the department all records, schedules and data
296 supporting this certificate for a period of five (5) years. To
297 the extent an insurer has identified areas, systems or processes
298 that require material improvement, updating or redesign, the
299 insurer shall document the identification and the remedial efforts
300 planned and underway to address such areas, systems or processes.
301 Such documentation must be available for inspection by the
302 commissioner.

303 **SECTION 5.** (1) If the licensee learns that a cybersecurity
304 event has or may have occurred, then the licensee, or an outside
305 vendor and/or service provider designated to act on behalf of the
306 licensee shall conduct a prompt investigation.

307 (2) During the investigation, the licensee, or an outside
308 vendor and/or service provider designated to act on behalf of the

309 licensee, shall, at a minimum, determine as much of the following
310 information as possible:

311 (a) Determine whether a cybersecurity event has
312 occurred;

313 (b) Assess the nature and scope of the cybersecurity
314 event;

315 (c) Identify any nonpublic information that may have
316 been involved in the cybersecurity event; and

317 (d) Perform or oversee reasonable measures to restore
318 the security of the information systems compromised in the
319 cybersecurity event in order to prevent further unauthorized
320 acquisition, release or use of nonpublic information in the
321 licensee's possession, custody or control.

322 (3) If the licensee learns that a cybersecurity event has or
323 may have occurred in a system maintained by a third-party service
324 provider, the licensee will complete the steps listed in
325 subsection (2) of this section or confirm and document that the
326 third-party service provider has completed those steps.

327 (4) The licensee shall maintain records concerning all
328 cybersecurity events for a period of at least five (5) years from
329 the date of the cybersecurity event and shall produce those
330 records upon demand of the commissioner.

331 **SECTION 6.** (1) Each licensee shall notify the commissioner
332 as promptly as possible but in no event later than three (3)
333 business days from a determination that a cybersecurity event
334 involving nonpublic information that is in the possession of a

335 licensee has occurred when either of the following criteria has
336 been met:

337 (a) This state is the licensee's state of domicile, in
338 the case of an insurer, or this state is the licensee's home
339 state, in the case of a producer, as those terms are defined in
340 Section 83-17-53, and the cybersecurity event has a reasonable
341 likelihood of materially harming a consumer residing in this state
342 or reasonable likelihood of materially harming any material part
343 of the normal operation(s) of the licensee; or

344 (b) The licensee reasonably believes that the nonpublic
345 information involved is of two hundred fifty (250) or more
346 consumers residing in this state and that is either of the
347 following:

348 (i) A cybersecurity event impacting the licensee
349 of which notice is required to be provided to any government body,
350 self-regulatory agency or any other supervisory body pursuant to
351 any state or federal law; or

352 (ii) A cybersecurity event that has a reasonable
353 likelihood of materially harming:

354 1. Any consumer residing in this state; or

355 2. Any material part of the normal

356 operation(s) of the licensee.

357 (2) The licensee shall provide as much of the following
358 information as possible. The licensee shall provide the
359 information in electronic form as directed by the commissioner.
360 The licensee shall have a continuing obligation to update and

361 supplement initial and subsequent notifications to the
362 commissioner regarding material changes to previously provided
363 information relating to the cybersecurity event.

364 (a) Date of the cybersecurity event;

365 (b) Description of how the information was exposed,
366 lost, stolen or breached, including the specific roles and
367 responsibilities of third-party service providers, if any;

368 (c) How the cybersecurity event was discovered;

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

371 (e) The identity of the source of the cybersecurity
372 event;

373 (f) Whether licensee has filed a police report or has
374 notified any regulatory, government or law enforcement agencies
375 and, if so, when such notification was provided;

376 (g) Description of the specific types of information
377 acquired without authorization. Specific types of information
378 means particular data elements including, for example, types of
379 medical information, types of financial information or types of
380 information allowing identification of the consumer;

381 (h) The period during which the information system was
382 compromised by the cybersecurity event;

383 (i) The number of total consumers in this state
384 affected by the cybersecurity event. The licensee shall provide
385 the best estimate in the initial report to the commissioner and

386 update this estimate with each subsequent report to the
387 commissioner pursuant to this section;

388 (j) The results of any internal review identifying a
389 lapse in either automated controls or internal procedures, or
390 confirming that all automated controls or internal procedures were
391 followed;

392 (k) Description of efforts being undertaken to
393 remediate the situation which permitted the cybersecurity event to
394 occur;

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

399 (m) Name of a contact person who is both familiar with
400 the cybersecurity event and authorized to act for the licensee.

401 (3) Licensee shall comply with Section 75-24-29, as
402 applicable, and provide a copy of the notice sent to consumers
403 under that statute to the commissioner, when a licensee is
404 required to notify the commissioner under subsection (1) of this
405 section.

406 (4) (a) In the case of a cybersecurity event in a system
407 maintained by a third-party service provider, of which the
408 licensee has become aware, the licensee shall treat such event as
409 it would under subsection (1) of this section unless the
410 third-party service provider provides the notice required under
411 subsection (1) of this section to the commissioner.

412 (b) The computation of licensee's deadlines shall begin
413 on the day after the third-party service provider notifies the
414 licensee of the cybersecurity event or the licensee otherwise has
415 actual knowledge of the cybersecurity event, whichever is sooner.

416 (c) Nothing in this act shall prevent or abrogate an
417 agreement between a licensee and another licensee, a third-party
418 service provider or any other party to fulfill any of the
419 investigation requirements imposed under Section 5 of this act or
420 notice requirements imposed under this section.

421 (5) (a) (i) In the case of a cybersecurity event involving
422 nonpublic information that is used by the licensee that is acting
423 as an assuming insurer or in the possession, custody or control of
424 a licensee that is acting as an assuming insurer and that does not
425 have a direct contractual relationship with the affected
426 consumers, the assuming insurer shall notify its affected ceding
427 insurers and the commissioner of its state of domicile within
428 three (3) business days of making the determination that a
429 cybersecurity event has occurred.

430 (ii) The ceding insurers that have a direct
431 contractual relationship with affected consumers shall fulfill the
432 consumer notification requirements imposed under Section 75-24-29
433 and any other notification requirements relating to a
434 cybersecurity event imposed under this section.

435 (b) (i) In the case of a cybersecurity event involving
436 nonpublic information that is in the possession, custody or
437 control of a third-party service provider of a licensee that is an

438 assuming insurer, the assuming insurer shall notify its affected
439 ceding insurers and the commissioner of its state of domicile
440 within three (3) business days of receiving notice from its
441 third-party service provider that a cybersecurity event has
442 occurred.

443 (ii) The ceding insurers that have a direct
444 contractual relationship with affected consumers shall fulfill the
445 consumer notification requirements imposed under Section 75-24-29
446 and any other notification requirements relating to a
447 cybersecurity event imposed under this section.

448 (c) Any licensee acting as assuming insurer shall have
449 no other notice obligations relating to a cybersecurity event or
450 other data breach under this section or any other law of this
451 state.

452 (6) In the case of a cybersecurity event involving nonpublic
453 information that is in the possession, custody or control of a
454 licensee that is an insurer or its third-party service provider
455 for which a consumer accessed the insurer's services through an
456 independent insurance producer, and for which consumer notice is
457 required under Section 75-24-29, the insurer shall notify the
458 producers of record of all affected consumers of the cybersecurity
459 event no later than the time at which notice is provided to the
460 affected consumers. The insurer is excused from this obligation
461 for any producers who are not authorized by law or contract to
462 sell, solicit or negotiate on behalf of the insurer, and in those

463 instances in which the insurer does not have the current producer
464 of record information for any individual consumer.

465 **SECTION 7.** (1) The commissioner shall have power to examine
466 and investigate into the affairs of any licensee to determine
467 whether the licensee has been or is engaged in any conduct in
468 violation of this act. This power is in addition to the powers
469 which the commissioner has under Section 83-5-201 et seq. Any
470 such investigation or examination shall be conducted pursuant to
471 Section 83-5-201 et seq.

472 (2) Whenever the commissioner has reason to believe that a
473 licensee has been or is engaged in conduct in this state which
474 violates this act, the commissioner may take action that is
475 necessary or appropriate to enforce the provisions of this act.

476 **SECTION 8.** (1) Any documents, materials or other
477 information in the control or possession of the department that
478 are furnished by a licensee or an employee or agent thereof acting
479 on behalf of a licensee pursuant to Section 4(9) of this act,
480 Section 6(2)(b), (c), (d), (e), (h), (j) and (k) of this act, or
481 that are obtained by the commissioner in an investigation or
482 examination pursuant to Section 7 of this act shall be
483 confidential by law and privileged, shall not be subject to the
484 Mississippi Public Records Act, shall not be subject to subpoena,
485 and shall not be subject to discovery or admissible in evidence in
486 any private civil action. However, the commissioner is authorized
487 to use the documents, materials or other information in the
488 furtherance of any regulatory or legal action brought as a part of

489 the commissioner's duties. The commissioner shall not otherwise
490 make the documents, materials or other information public without
491 the prior written consent of the licensee.

492 (2) Neither the commissioner nor any person who received
493 documents, materials or other information while acting under the
494 authority of the commissioner shall be permitted or required to
495 testify in any private civil action concerning any confidential
496 documents, materials or information subject to subsection (1) of
497 this section.

498 (3) In order to assist in the performance of the
499 commissioner's duties under this act, the commissioner:

500 (a) May share documents, materials or other
501 information, including the confidential and privileged documents,
502 materials or information subject to subsection (1) of this
503 section, with other state, federal and international regulatory
504 agencies, with the National Association of Insurance
505 Commissioners, its affiliates or subsidiaries, and with state,
506 federal and international law enforcement authorities, provided
507 that the recipient agrees in writing to maintain the
508 confidentiality and privileged status of the document, material or
509 other information;

510 (b) May receive documents, materials or information,
511 including otherwise confidential and privileged documents,
512 materials or information, from the National Association of
513 Insurance Commissioners, its affiliates or subsidiaries and from
514 regulatory and law enforcement officials of other foreign or

515 domestic jurisdictions, and shall maintain as confidential or
516 privileged any document, material or information received with
517 notice or the understanding that it is confidential or privileged
518 under the laws of the jurisdiction that is the source of the
519 document, material or information; and

520 (c) May share documents, materials or other information
521 subject to subsection (1) of this section, with a third-party
522 consultant or vendor provided the consultant agrees in writing to
523 maintain the confidentiality and privileged status of the
524 document, material or other information.

525 (d) May enter into agreements governing sharing and use
526 of information consistent with this subsection (3).

527 (4) No waiver of any applicable privilege or claim of
528 confidentiality in the documents, materials, or information shall
529 occur as a result of disclosure to the commissioner under this
530 section or as a result of sharing as authorized in subsection (3)
531 of this section.

532 (5) Nothing in this act shall prohibit the commissioner from
533 releasing final, adjudicated actions that are open to public
534 inspection pursuant to the Mississippi Public Records Act, to a
535 database or other clearinghouse service maintained by the National
536 Association of Insurance Commissioners, its affiliates or
537 subsidiaries.

538 (6) Documents, materials or other information in the
539 possession or control of the National Association of Insurance
540 Commissioners or a third-party consultant or vendor pursuant to

541 this act shall be confidential by law and privileged, shall not be
542 subject to the Mississippi Public Records Act, shall not be
543 subject to subpoena, and shall not be subject to discovery or
544 admissible in evidence in any private civil action.

545 **SECTION 9.** (1) The following exceptions shall apply to this
546 act:

547 (a) A licensee meeting any of the following criteria is
548 exempt from Sections 4, 5(3) and 6(4)(a) and (b) of this act:

549 (i) Fewer than fifty (50) employees, excluding any
550 independent contractors;

551 (ii) Less than Five Million Dollars
552 (\$5,000,000.00) in gross annual revenue;

553 (iii) Less than Ten Million Dollars
554 (\$10,000,000.00) in year-end total assets; or

555 (iv) Insurance producers and adjusters.

556 (b) A licensee subject to Public Law 104-191, 110 Stat.
557 1936, enacted August 21, 1996, (Health Insurance Portability and
558 Accountability Act) that has established and maintains an
559 information security program pursuant to such statutes, rules,
560 regulations, procedures or guidelines established thereunder, will
561 be considered to meet the requirements of Section 4 of this act,
562 provided that licensee is compliant with, and submits a written
563 statement certifying its compliance with, the same;

564 (c) An employee, agent, representative or designee of a
565 licensee, who is also a licensee, is exempt from Section 4 of this
566 act and need not develop its own information security program to

567 the extent that the employee, agent, representative or designee is
568 covered by the information security program of the other licensee.

569 (d) A licensee affiliated with a depository institution
570 that maintains an information security program in compliance with
571 the *Interagency Guidelines Establishing Standards for Safeguarding*
572 *Customer Information* as set forth pursuant to Sections 501 and 505
573 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) shall be
574 considered to meet the requirements of Section 4, provided that
575 the licensee produces, upon request, documentation satisfactory to
576 the commissioner that independently validates the affiliated
577 depository institution's adoption of an information security
578 program that satisfies the Interagency Guidelines.

579 (2) In the event that a licensee ceases to qualify for an
580 exception, such licensee shall have one hundred eighty (180) days
581 to comply with this act.

582 **SECTION 10.** In the case of a violation of this act, a
583 licensee may be penalized in accordance with Section 83-5-85.

584 **SECTION 11.** The commissioner may issue such regulations as
585 shall be necessary to carry out the provisions of this act.

586 **SECTION 12.** If any provisions of this act or the application
587 thereof to any person or circumstance is for any reason held to be
588 invalid, the remainder of the act and the application of such
589 provision to other persons or circumstances shall not be affected
590 thereby.

591 **SECTION 13.** Licensees shall have one (1) year from the
592 effective date of this act to implement Section 4 of this act and

593 two (2) years from the effective date of this act to implement
594 Section 4(6) of this act.

595 **SECTION 14.** This act shall take effect and be in force from
596 and after July 1, 2019.

**Further, amend by striking the title in its entirety and
inserting in lieu thereof the following:**

1 AN ACT TO ESTABLISH THE INSURANCE DATA SECURITY LAW; TO
2 PROVIDE THE PURPOSE AND INTENT OF THE ACT; TO DEFINE CERTAIN TERMS
3 USED IN THE ACT; TO REQUIRE INSURANCE LICENSEES IN THIS STATE TO
4 DEVELOP, IMPLEMENT AND MAINTAIN AN INFORMATION SECURITY PROGRAM;
5 TO REQUIRE CERTAIN INVESTIGATION OF A CYBERSECURITY EVENT; TO
6 REQUIRE CERTAIN NOTIFICATION OF A CYBERSECURITY EVENT; TO PROVIDE
7 FOR CERTAIN CONFIDENTIALITY; TO PROVIDE EXCEPTIONS TO THE ACT; TO
8 PROVIDE FOR PENALTIES FOR VIOLATIONS OF THE ACT; TO PROVIDE THE
9 COMMISSIONER OF INSURANCE WITH REGULATORY POWERS NECESSARY TO
10 CARRY OUT THE ACT; AND FOR RELATED PURPOSES.

HR43\SB2831A.J

Andrew Ketchings
Clerk of the House of Representatives