

Date: (Filing No. S-)

HEALTH COVERAGE, INSURANCE AND FINANCIAL SERVICES

Reproduced and distributed under the direction of the Secretary of the Senate.

**STATE OF MAINE
SENATE
129TH LEGISLATURE
SECOND SPECIAL SESSION**

COMMITTEE AMENDMENT “ ” to S.P. 697, L.D. 1995, Bill, “An Act To Enact the Maine Insurance Data Security Act”

Amend the bill in section 1 in §2262 in the first paragraph in the first line (page 1, line 8 in L.D.) by inserting after the following: "and" the following: 'exclusive'

Amend the bill in section 1 in §2263 by striking out all of subsection 1 (page 1, lines 16 to 19 in L.D.) and inserting the following:

1. Authorized individual. "Authorized individual" means an individual whose access to the nonpublic information held by the licensee and its information systems is authorized and determined by the licensee to be necessary and appropriate.'

Amend the bill in section 1 in §2263 by striking out all of subsection 7 (page 2, lines 10 to 12 in L.D.) and inserting the following:

7. Insurance carrier. "Insurance carrier" has the same meaning as in section 2204, subsection 15.'

Amend the bill in section 1 in §2263 in subsection 10 by inserting at the end a new blocked paragraph to read:

"Nonpublic information" does not include a consumer's personally identifiable information that has been anonymized using a method no less secure than the safe harbor method under the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.'

Amend the bill in section 1 in §2264 in subsection 2 in paragraph B in the first line (page 3, line 36 in L.D.) by inserting after the following: "against" the following: 'reasonably foreseeable'

Amend the bill in section 1 in §2264 in subsection 6 in paragraph B in the last line (page 6, line 16 in L.D.) by inserting after the following: "accessible" the following: 'to'

Amend the bill in section 1 in §2264 in subsection 9 in the first line (page 7, line 1 in L.D.) by striking out the following: "February" and inserting the following: 'April'

COMMITTEE AMENDMENT

1 Amend the bill in section 1 in §2265 by striking out all of subsection 2 (page 7, lines
2 25 to 28 in L.D.) and inserting the following:

3 **2. System maintained by 3rd-party service provider.** If a licensee learns that a
4 cybersecurity event has or may have occurred in an information system maintained by a
5 3rd-party service provider, the licensee shall either use its best efforts to complete the
6 steps listed in subsection 1 or confirm that the 3rd-party service provider has completed
7 those steps.'

8 Amend the bill in section 1 in §2266 in subsection 1 in the 3rd line (page 7, line 35 in
9 L.D.) by striking out the following: "72 hours" and inserting the following: '3 business
10 days'

11 Amend the bill in section 1 in §2266 in subsection 5 in paragraph A in subparagraph
12 (1) in the 2nd line (page 9, line 32 in L.D.) by striking out the following: "72 hours" and
13 inserting the following: '3 business days'

14 Amend the bill in section 1 in §2266 in subsection 5 in paragraph B in subparagraph
15 (1) in the 2nd line (page 10, line 2 in L.D.) by striking out the following: "72 hours" and
16 inserting the following: '3 business days'

17 Amend the bill in section 1 in §2266 in subsection 6 in the 6th line (page 10, line 13
18 in L.D.) by striking out the following: "as soon as practicable" and inserting the
19 following: 'no later than the time consumers must be notified under subsection 3 or'

20 Amend the bill in section 1 in §2269 in subsection 1 in the last line (page 11, line 12
21 in L.D.) by inserting after the following: "contractors" the following: 'working for the
22 licensee in the business of insurance'

23 Amend the bill in section 1 in §2269 by striking out all of subsection 2 (page 11, lines
24 13 to 18 in L.D.) and inserting the following:

25 **2. Licensees subject to federal law.** The following provisions apply to licensees
26 subject to federal law.

27 A. A licensee that is subject to and in compliance with the federal Health Insurance
28 Portability and Accountability Act of 1996, Public Law 104-191 and related privacy,
29 security and breach notification regulations pursuant to 45 Code of Federal
30 Regulations, Parts 160 and 164 and the Health Information Technology for Economic
31 and Clinical Health Act, Public Law 111-5 is considered to meet the requirements of
32 this chapter, other than the requirements of section 2266, subsection 1 for notice to
33 the superintendent, if:

34 (1) The licensee maintains a program for information security and breach
35 notification that treats all nonpublic information relating to consumers in this
36 State in the same manner as protected health information;

37 (2) The licensee annually submits to the superintendent a written statement
38 certifying that the licensee is in compliance with the requirements of this
39 paragraph; and

40 (3) The superintendent has not issued a determination finding that the applicable
41 federal regulations are materially less stringent than the requirements of this
42 chapter.

1 B. A licensee that is a producer business entity owned by a depository institution and
2 maintains an information security program in compliance with the standards for
3 safeguarding customer information as set forth pursuant to the Gramm-Leach-Bliley
4 Act, 15 United States Code, Sections 6801 and 6805 is considered to meet the
5 requirements of section 2264 if:

6 (1) Upon request, the licensee produces documentation satisfactory to the
7 superintendent that independently validates the controlling depository
8 institution's adoption of an information security program that satisfies the
9 standards for safeguarding customer information;

10 (2) The licensee annually submits to the superintendent a written statement
11 certifying that the licensee is in compliance with the requirements of this
12 paragraph; and

13 (3) The superintendent has not issued a determination finding that the standards
14 for safeguarding customer information are materially less stringent than the
15 requirements of section 2264.'

16 Amend the bill in section 1 in §2272 in the first paragraph in the first line (page 11,
17 line 34 in L.D.) by striking out the following: "January" and inserting the following:
18 'June'

19 Amend the bill in section 1 in §2272 in the first paragraph in the 2nd line (page 11,
20 line 35 in L.D.) by striking out the following: "January" and inserting the following:
21 'June'

22 Amend the bill by relettering or renumbering any nonconsecutive Part letter or
23 section number to read consecutively.

24 SUMMARY

25 This amendment makes the following changes to the bill.

26 1. It clarifies the definitions of "authorized individual," "insurance carrier" and
27 "nonpublic information."

28 2. It extends the time period for notification of a cybersecurity event from 72 hours
29 to no later than 3 business days.

30 3. It changes the date that an insurance carrier annually certify compliance with the
31 requirements for an information security program from February 15th to April 15th.

32 4. It clarifies the exemption for small business licensees and for certain licensees
33 subject to federal law.

34 5. It changes the effective date to June 1, 2021.

35 FISCAL NOTE REQUIRED

36 (See attached)