

**PROPOSED AMENDMENTS TO
SENATE BILL 601**

1 On page 1 of the printed bill, line 3, delete “646A.602 and 646A.604” and
2 insert “646A.602, 646A.604 and 646A.622”.

3 On page 2 , line 8, restore “in combination with” and delete the boldfaced
4 material.

5 Delete lines 21 through 24 and insert:

6 “(E) Data from automatic measurements of a consumer’s physical char-
7 acteristics, such as an image of a fingerprint, retina or iris, that are used
8 to authenticate the consumer’s identity in the course of a financial trans-
9 action or other transaction;

10 “(F) A consumer’s health insurance policy number or health insurance
11 subscriber identification number in combination with any other unique
12 identifier that a health insurer uses to identify the consumer; or

13 “(G) Any information about a consumer’s medical history or mental or
14 physical condition or about a health care professional’s medical diagnosis
15 or treatment of the consumer.”.

16 On page 3, line 20, delete “, maintains or otherwise possesses” and insert
17 “or licenses”.

18 In line 38, delete “100” and insert “250”.

19 In line 40, after “of” insert “, or under license of”.

20 In line 42, delete “and the Attorney General”.

21 In line 44, delete the boldfaced material.

22 In line 45, after “person” insert “that owns or licenses personal informa-

1 tion”.

2 On page 4, line 8, after “person” insert “that owns or licenses personal
3 information”.

4 In line 24, delete “and social media sites”.

5 In line 25, delete “or a presence on a social media site”.

6 In line 32, delete the comma.

7 In line 33, delete “maintained, licensed or possessed” and insert “or li-
8 censed”.

9 On page 5, line 13, delete “breach of security procedures” and insert
10 “procedures for a breach of security”.

11 In lines 14 through 16, delete the boldfaced material and insert “the
12 person’s primary or functional federal regulator adopts, promulgates or is-
13 sues in rules, regulations, procedures, guidelines or guidance, if the rules,
14 regulations, procedures, guidelines or guidance” and restore the bracketed
15 material.

16 In lines 23 and 24, delete the boldfaced material and insert “disclosure
17 requirements at least as thorough as the protections and disclosure require-
18 ments provided under”.

19 After line 27, insert:

20 “(d)(A) Except as provided in subparagraph (B) of this paragraph, a cov-
21 ered entity, as defined in 45 C.F.R. 160.103, as in effect on the effective date
22 of this 2015 Act, that is governed under 45 C.F.R. parts 160 and 164, as in
23 effect on the effective date of this 2015 Act, if the covered entity sends the
24 Attorney General a copy of the notice the covered entity sent to consumers
25 under ORS 646A.604 or a copy of the notice that the covered entity sent to
26 the primary functional regulator designated for the covered entity under the
27 Health Insurance Portability and Availability Act of 1996, (P.L. 104-191, 110
28 Stat. 1936, 42 U.S.C. 300(gg), 29 U.S.C. 118 et seq., 42 U.S.C. 1320(d) et seq.,
29 45 C.F.R. parts 160 and 164).

30 “(B) A covered entity is subject to the provisions of this section if the

1 covered entity does not send a copy of a notice described in subparagraph
2 (A) of this paragraph to the Attorney General within a reasonable time after
3 the Attorney General requests the copy.”.

4 In line 29, delete “that is subject to enforcement under ORS 646.632”.

5 After line 31, insert:

6 **“SECTION 3.** ORS 646A.622 is amended to read:

7 “646A.622. (1) [*Any*] **A person** that owns, maintains or otherwise possesses
8 data that includes a consumer’s personal information that [*is used*] **the**
9 **person uses** in the course of the person’s business, vocation, occupation or
10 volunteer activities [*must*] **shall** develop, implement and maintain reasonable
11 safeguards to protect the security, confidentiality and integrity of the per-
12 sonal information, [*including disposal of the data*] **including safeguards**
13 **that protect the personal information when the person disposes of the**
14 **personal information.**

15 “(2) [*The following shall be deemed in compliance*] **A person complies**
16 with subsection (1) of this section **if the person:**

17 “(a) [*A person that*] **Complies** with a state or federal law [*providing*] **that**
18 **provides** greater protection to personal information than [*that provided by*]
19 **the protections that** this section **provides.**

20 “(b) [*A person that is subject to and*] **Complies** with regulations
21 promulgated [*pursuant to*] **under** Title V of the Gramm-Leach-Bliley Act of
22 1999 (15 U.S.C. 6801 to 6809) as [*that Act existed on October 1, 2007*] **in effect**
23 **on the effective date of this 2015 Act, if the person is subject to the**
24 **Act.**

25 “(c) [*A person that is subject to and*] **Complies** with regulations [*imple-*
26 *menting*] **that implement** the Health Insurance Portability and Account-
27 ability Act of 1996 (45 C.F.R. parts 160 and 164) as [*that Act existed on*
28 *October 1, 2007*] **in effect on the effective date of this 2015 Act, if the**
29 **person is subject to the Act.**

30 “(d) [*A person that*] **Implements** an information security program that in-

1 cludes *[the following]*:

2 “(A) Administrative safeguards such as *[the following, in which the*
3 *person]*:

4 “(i) *[Designates]* **Designating** one or more employees to coordinate the
5 security program;

6 “(ii) *[Identifies]* **Identifying** reasonably foreseeable internal and external
7 risks;

8 “(iii) *[Assesses the sufficiency of]* **Assessing whether existing** safeguards
9 *[in place to]* **adequately** control the identified risks;

10 “(iv) *[Trains and manages employees in the]* **Training and managing**
11 **employees in** security program practices and procedures;

12 “(v) *[Selects]* **Selecting** service providers **that are** capable of maintaining
13 appropriate safeguards, and *[requires those safeguards by contract]* **requiring**
14 **the service providers by contract to maintain the safeguards;** and

15 “(vi) *[Adjusts]* **Adjusting** the security program in light of business
16 changes or new circumstances;

17 “(B) Technical safeguards such as *[the following, in which the person]*:

18 “(i) *[Assesses]* **Assessing** risks in network and software design;

19 “(ii) *[Assesses]* **Assessing** risks in information processing, transmission
20 and storage;

21 “(iii) *[Detects, prevents and responds]* **Detecting, preventing and re-**
22 **sponding** to attacks or system failures; and

23 “(iv) *[Regularly tests and monitors]* **Testing and monitoring regularly**
24 the effectiveness of key controls, systems and procedures; and

25 “(C) Physical safeguards such as *[the following, in which the person]*:

26 “(i) *[Assesses]* **Assessing** risks of information storage and disposal;

27 “(ii) *[Detects, prevents and responds]* **Detecting, preventing and re-**
28 **sponding** to intrusions;

29 “(iii) *[Protects]* **Protecting** against unauthorized access to or use of per-
30 sonal information during or after *[the collection, transportation and de-*

1 *struction or disposal of the]* **collecting, transporting, destroying or**
2 **disposing of the personal** information; and

3 “(iv) [*Disposes*] **Disposing** of personal information after [*it is no longer*
4 *needed*] **the person no longer needs the personal information** for busi-
5 ness purposes or as required by local, state or federal law by burning,
6 pulverizing, shredding or modifying a physical record and by destroying or
7 erasing electronic media so that the information cannot be read or recon-
8 structed.

9 “(3) A person complies with subsection (2)(d)(C)(iv) of this section if the
10 person contracts with another person engaged in the business of record de-
11 struction to dispose of personal information in a manner **that is** consistent
12 with subsection (2)(d)(C)(iv) of this section.

13 “(4) Notwithstanding subsection (2) of this section, a person that is an
14 owner of a small business as defined in ORS 285B.123 (2) complies with
15 subsection (1) of this section if the person’s information security and disposal
16 program contains administrative, technical and physical safeguards and dis-
17 posal measures **that are** appropriate [*to*] **for** the size and complexity of the
18 small business, the nature and scope of [*its*] **the small business’s** activities,
19 and the sensitivity of the personal information [*collected*] **the small busi-**
20 **ness collects** from or about consumers.”.

21 In line 32, delete “3” and insert “4”.

22 On page 6, delete lines 5 through 7 and insert:

23 “**SECTION 5.** The amendments to ORS 646.607, 646A.602, 646A.604 and
24 646A.622 by sections 1 to 4 of this 2015 Act apply to breaches of security that
25 occur on or after the effective date of this 2015 Act.”.

26
