

**A-Engrossed**  
**Senate Bill 684**

Ordered by the Senate March 29  
Including Senate Amendments dated March 29

Sponsored by COMMITTEE ON JUDICIARY

**SUMMARY**

The following summary is not prepared by the sponsors of the measure and is not a part of the body thereof subject to consideration by the Legislative Assembly. It is an editor's brief statement of the essential features of the measure.

Specifies requirements for covered entities that own, license, maintain, store, manage, collect, process, acquire or otherwise possess personal information, and for vendors that provide services to covered entities, to notify consumers of breach of security. Specifies exemptions for certain covered entities that are subject to other laws governing protections and disclosures.

**A BILL FOR AN ACT**

1  
2 Relating to actions with respect to a breach of security that involves personal information; creating  
3 new provisions; and amending ORS 646A.600, 646A.602, 646A.604 and 646A.622.

4 **Be It Enacted by the People of the State of Oregon:**

5 **SECTION 1.** ORS 646A.600 is amended to read:

6 646A.600. ORS 646A.600 to 646A.628 shall be known as the Oregon Consumer *[Identity Theft]*  
7 **Information** Protection Act.

8 **SECTION 2.** ORS 646A.602, as amended by section 1, chapter 10, Oregon Laws 2018, is amended  
9 to read:

10 646A.602. As used in ORS 646A.600 to 646A.628:

11 (1)(a) "Breach of security" means an unauthorized acquisition of computerized data that mate-  
12 rially compromises the security, confidentiality or integrity of personal information that a person  
13 maintains **or possesses**.

14 (b) "Breach of security" does not include an inadvertent acquisition of personal information by  
15 a person or the person's employee or agent if the personal information is not used in violation of  
16 applicable law or in a manner that harms or poses an actual threat to the security, confidentiality  
17 or integrity of the personal information.

18 (2) "Consumer" means an individual resident of this state.

19 (3) "Consumer report" means a consumer report as described in section 603(d) of the federal Fair  
20 Credit Reporting Act (15 U.S.C. 1681a(d)), as that Act existed on *[June 2, 2018]* **the effective date**  
21 **of this 2019 Act**, that a consumer reporting agency compiles and maintains.

22 (4) "Consumer reporting agency" means a consumer reporting agency as described in section  
23 603(p) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(p)) as that Act existed on *[June 2,*  
24 *2018]* **the effective date of this 2019 Act**.

25 (5)(a) "**Covered entity**" means a person that owns, licenses, maintains, stores, manages,  
26 collects, processes, acquires or otherwise possesses personal information in the course of the  
27 person's business, vocation, occupation or volunteer activities.

**NOTE:** Matter in **boldfaced** type in an amended section is new; matter *[italic and bracketed]* is existing law to be omitted.  
New sections are in **boldfaced** type.

1       **(b) “Covered entity” does not include a person described in paragraph (a) of this sub-**  
2 **section to the extent that the person acts solely as a vendor.**

3       [(5)] **(6)** “Debt” means any obligation or alleged obligation arising out of a consumer transaction.

4       [(6)] **(7)** “Encryption” means an algorithmic process that renders data unreadable or unusable  
5 without the use of a confidential process or key.

6       [(7)] **(8)** “Extension of credit” means a right to defer paying debt or a right to incur debt and  
7 defer paying the debt, that is offered or granted primarily for personal, family or household pur-  
8 poses.

9       [(8)] **(9)** “Identity theft” has the meaning set forth in ORS 165.800.

10       [(9)] **(10)** “Identity theft declaration” means a completed and signed statement that documents  
11 alleged identity theft, using a form available from the Federal Trade Commission, or another sub-  
12 stantially similar form.

13       [(10)] **(11)** “Person” means an individual, private or public corporation, partnership, cooperative,  
14 association, estate, limited liability company, organization or other entity, whether or not organized  
15 to operate at a profit, or a public body as defined in ORS 174.109.

16       [(11)(a)] **(12)(a)** “Personal information” means:

17       (A) A consumer’s first name or first initial and last name in combination with any one or more  
18 of the following data elements, if encryption, redaction or other methods have not rendered the data  
19 elements unusable or if the data elements are encrypted and the encryption key has been acquired:

20       (i) A consumer’s Social Security number;

21       (ii) A consumer’s driver license number or state identification card number issued by the De-  
22 partment of Transportation;

23       (iii) A consumer’s passport number or other identification number issued by the United States;

24       (iv) A consumer’s financial account number, credit card number or debit card number, in com-  
25 bination with any required security code, access code or password that would permit access to a  
26 consumer’s financial account, or any other information or combination of information that a person  
27 reasonably knows or should know would permit access to the consumer’s financial account;

28       (v) Data from automatic measurements of a consumer’s physical characteristics, such as an im-  
29 age of a fingerprint, retina or iris, that are used to authenticate the consumer’s identity in the  
30 course of a financial transaction or other transaction;

31       (vi) A consumer’s health insurance policy number or health insurance subscriber identification  
32 number in combination with any other unique identifier that a health insurer uses to identify the  
33 consumer; *[and]* **or**

34       (vii) Any information about a consumer’s medical history or mental or physical condition or  
35 about a health care professional’s medical diagnosis or treatment of the consumer.

36       **(B) A user name or other means of identifying a consumer for the purpose of permitting**  
37 **access to the consumer’s account, together with any other method necessary to authenticate**  
38 **the user name or means of identification.**

39       [(B)] **(C)** Any of the data elements or any combination of the data elements described in sub-  
40 paragraph (A) **or (B)** of this paragraph without the consumer’s **user name, or the consumer’s** first  
41 name or first initial and last name, if:

42       (i) Encryption, redaction or other methods have not rendered the data element or combination  
43 of data elements unusable; and

44       (ii) The data element or combination of data elements would enable a person to commit identity  
45 theft against a consumer.

1 (b) "Personal information" does not include information in a federal, state or local government  
2 record, other than a Social Security number, that is lawfully made available to the public.

3 [(12)] (13) "Proper identification" means written information or documentation that a consumer  
4 or representative can present to another person as evidence of the consumer's or representative's  
5 identity, examples of which include:

6 (a) A valid Social Security number or a copy of a valid Social Security card;

7 (b) A certified or otherwise official copy of a birth certificate that a governmental body issued;  
8 and

9 (c) A copy of a driver license or other government-issued identification.

10 [(13)] (14) "Protected consumer" means an individual who is:

11 (a) Not older than 16 years old at the time a representative requests a security freeze on the  
12 individual's behalf; or

13 (b) Incapacitated or for whom a court or other authority has appointed a guardian or  
14 conservator.

15 [(14)] (15) "Protective record" means information that a consumer reporting agency compiles to  
16 identify a protected consumer for whom the consumer reporting agency has not prepared a consumer  
17 report.

18 [(15)] (16) "Redacted" means altered or truncated so that no more than the last four digits of  
19 a Social Security number, driver license number, state identification card number, passport number  
20 or other number issued by the United States, financial account number, credit card number or debit  
21 card number is visible or accessible.

22 [(16)] (17) "Representative" means a consumer who provides a consumer reporting agency with  
23 sufficient proof of the consumer's authority to act on a protected consumer's behalf.

24 [(17)] (18) "Security freeze" means a notice placed in a consumer report at a consumer's request  
25 or a representative's request or in a protective record at a representative's request that, subject to  
26 certain exemptions, prohibits a consumer reporting agency from releasing information in the con-  
27 sumer report or the protective record for an extension of credit, unless the consumer temporarily  
28 lifts the security freeze on the consumer's consumer report or a protected consumer or represen-  
29 tative removes the security freeze on or deletes the protective record.

30 (19) "**Vendor**" means a person with which a covered entity contracts to maintain, store,  
31 manage, process or otherwise access personal information for the purpose of, or in con-  
32 nection with, providing services to or on behalf of the covered entity.

33 **SECTION 3.** ORS 646A.604, as amended by section 2, chapter 10, Oregon Laws 2018, is amended  
34 to read:

35 646A.604. (1) If a *[person owns, licenses or otherwise possesses personal information that the per-*  
36 *son uses in the course of the person's business, vocation, occupation or volunteer activities and that*  
37 *was]* **covered entity is** subject to a breach of security or *[if the person received]* **receives** notice of  
38 a breach of security from *[another person that maintains or otherwise possesses personal information*  
39 *on the person's behalf]* **a vendor**, the *[person]* **covered entity** shall give notice of the breach of se-  
40 curity to:

41 (a) The consumer to whom the personal information pertains.

42 (b) The Attorney General, either in writing or electronically, if the number of consumers to  
43 whom the *[person]* **covered entity** must send the notice described in paragraph (a) of this subsection  
44 exceeds 250.

45 [(2) *A person that maintains or otherwise possesses personal information on behalf of another*

1 *person that is described in subsection (1) of this section shall notify the other person as soon as is*  
2 *practicable after discovering a breach of security.]*

3 **(2)(a) A vendor that discovers a breach of security or has reason to believe that a breach**  
4 **of security has occurred shall notify a covered entity with which the vendor has a contract**  
5 **as soon as is practicable but not later than 10 days after discovering the breach of security**  
6 **or having a reason to believe that the breach of security occurred.**

7 **(b) If a vendor has a contract with another vendor that, in turn, has a contract with a**  
8 **covered entity, the vendor shall notify the other vendor of a breach of security as provided**  
9 **in paragraph (a) of this subsection.**

10 **(c) A vendor shall notify the Attorney General in writing or electronically if the vendor**  
11 **was subject to a breach of security that involved the personal information of more than 250**  
12 **consumers or a number of consumers that the vendor could not determine. This paragraph**  
13 **does not apply to the vendor if the covered entity described in paragraph (a) or (b) of this**  
14 **subsection has notified the Attorney General in accordance with the requirements of this**  
15 **section.**

16 **(3)(a)** *[Except as provided in paragraph (b) of this subsection, a person that must give notice of a*  
17 *breach of security under this section shall give the notice]* **A covered entity shall give notice of a**  
18 **breach of security** in the most expeditious manner possible, without unreasonable delay, but not  
19 later than 45 days after discovering or receiving notification of the breach of security.

20 **(b)** *[In* **Before** *providing the notice* **described in paragraph (a) of this subsection,** *[the*  
21 *person]* **a covered entity** shall undertake reasonable measures that are necessary to:

22 (A) Determine sufficient contact information for the intended recipient of the notice;

23 (B) Determine the scope of the breach of security; and

24 (C) Restore the reasonable integrity, security and confidentiality of the personal information.

25 *[(b)]* **(c)** *A* *[person that must give notice of a breach of security under this section]* **covered entity**  
26 may delay giving the notice **described in paragraph (a) of this subsection** only if a law enforce-  
27 ment agency determines that a notification will impede a criminal investigation and if the law  
28 enforcement agency requests in writing that the *[person]* **covered entity** delay the notification.

29 **(4)** *A* *[person that must give notice under this section to a consumer]* **covered entity** may notify  
30 *[the]* **a consumer** of a breach of security:

31 (a) In writing;

32 (b) Electronically, if the *[person]* **covered entity** customarily communicates with the consumer  
33 electronically or if the notice is consistent with the provisions regarding electronic records and  
34 signatures set forth in the Electronic Signatures in Global and National Commerce Act (15 U.S.C.  
35 7001) as that Act existed on *[June 2, 2018]* **the effective date of this 2019 Act;**

36 (c) By telephone, if the *[person]* **covered entity** contacts the affected consumer directly; or

37 (d) With substitute notice, if the *[person]* **covered entity** demonstrates that the cost of notifi-  
38 cation otherwise would exceed \$250,000 or that the affected class of consumers exceeds 350,000, or  
39 if the *[person]* **covered entity** does not have sufficient contact information to notify affected con-  
40 sumers. For the purposes of this paragraph, “substitute notice” means:

41 (A) Posting the notice or a link to the notice conspicuously on the *[person’s]* **covered entity’s**  
42 website if the *[person]* **covered entity** maintains a website; and

43 (B) Notifying major statewide television and newspaper media.

44 **(5)** Notice under this section must include, at a minimum:

45 (a) A description of the breach of security in general terms;

1 (b) The approximate date of the breach of security;

2 (c) The type of personal information that was subject to the breach of security;

3 (d) Contact information for the *[person that gave the notice]* **covered entity**;

4 (e) Contact information for national consumer reporting agencies; and

5 (f) Advice to the consumer to report suspected identity theft to law enforcement, including the  
6 Attorney General and the Federal Trade Commission.

7 (6) If a *[person]* **covered entity** discovers **or receives notice of** a breach of security that affects  
8 more than 1,000 consumers, the *[person]* **covered entity** shall notify, without unreasonable delay,  
9 all consumer reporting agencies that compile and maintain reports on consumers on a nationwide  
10 basis of the timing, distribution and content of the notice the *[person]* **covered entity** gave to af-  
11 fected consumers and shall include in the notice any police report number assigned to the breach  
12 of security. A *[person]* **covered entity** may not delay notifying affected consumers of a breach of  
13 security in order to notify consumer reporting agencies.

14 (7)(a) If a *[person]* **covered entity** must notify a consumer of a breach of security under this  
15 section, and in connection with the notification the *[person]* **covered entity or an agent or affiliate**  
16 **of the covered entity** offers to provide credit monitoring services or identity theft prevention and  
17 mitigation services without charge to the consumer, the *[person]* **covered entity, the agent or the**  
18 **affiliate** may not condition the *[person's]* provision of the services on the consumer's providing the  
19 *[person]* **covered entity, the agent or the affiliate** with a credit or debit card number or on the  
20 consumer's acceptance of any other service the *[person]* **covered entity** offers to provide for a fee.

21 (b) If a *[person]* **covered entity or an agent or affiliate of the covered entity** offers additional  
22 credit monitoring services or identity theft prevention and mitigation services for a fee to a con-  
23 sumer under the circumstances described in paragraph (a) of this subsection, the *[person]* **covered**  
24 **entity, the agent or the affiliate** must separately, distinctly, clearly and conspicuously disclose in  
25 the offer for the additional credit monitoring services or identity theft prevention and mitigation  
26 services that the *[person]* **covered entity, the agent or the affiliate** will charge the consumer a  
27 fee.

28 (c) The terms and conditions of any contract under which one person offers or provides credit  
29 monitoring services or identity theft prevention and mitigation services on behalf of another person  
30 under the circumstances described in paragraph (a) of this subsection must require compliance with  
31 the requirements of paragraphs (a) and (b) of this subsection.

32 (8) Notwithstanding subsection (1) of this section, a *[person]* **covered entity** does not need to  
33 notify consumers of a breach of security if, after an appropriate investigation or after consultation  
34 with relevant federal, state or local law enforcement agencies, the *[person]* **covered entity** reason-  
35 ably determines that the consumers whose personal information was subject to the breach of secu-  
36 rity are unlikely to suffer harm. The *[person]* **covered entity** must document the determination in  
37 writing and maintain the documentation for at least five years.

38 (9) This section does not apply to:

39 (a) **Personal information that is subject to, and** a person that complies with, notification re-  
40 quirements or procedures for a breach of security that the person's primary or functional federal  
41 regulator adopts, promulgates or issues in rules, regulations, procedures, guidelines or guidance, if  
42 the *[rules, regulations, procedures, guidelines or guidance provides greater protection to personal in-*  
43 *formation and disclosure requirements at least as thorough as the protections and disclosure require-*  
44 *ments provided under this section]* **personal information and the person would otherwise be**  
45 **subject to ORS 646A.600 to 646A.628.**

1 (b) **Personal information that is subject to, and** a person that complies with, a state or fed-  
 2 eral law that provides greater protection to personal information and disclosure requirements at  
 3 least as thorough as the protections and disclosure requirements provided under this section.

4 (c) [A person] **A covered entity or vendor** that [is subject to and] complies with regulations  
 5 promulgated [pursuant to] **under** Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to  
 6 6809) as that Act existed on [June 2, 2018] **the effective date of this 2019 Act, if personal infor-**  
 7 **mation that is subject to ORS 646A.600 to 646A.628 is also subject to that Act.**

8 [(d)(A) *Except as provided in subparagraph (B) of this paragraph, a covered entity, as defined in*  
 9 *45 C.F.R. 160.103, as in effect on June 2, 2018, that is governed under 45 C.F.R. parts 160 and 164,*  
 10 *as in effect on June 2, 2018, if the covered entity sends the Attorney General a copy of the notice the*  
 11 *covered entity sent to consumers under this section or a copy of the notice that the covered entity sent*  
 12 *to the primary functional regulator designated for the covered entity under the Health Insurance Por-*  
 13 *tability and Availability Act of 1996, (P.L. 104-191, 110 Stat. 1936, 42 U.S.C. 300(gg), 29 U.S.C. 118*  
 14 *et seq., 42 U.S.C. 1320(d) et seq., 45 C.F.R. parts 160 and 164).]*

15 [(B) *A covered entity is subject to the provisions of this section if the covered entity does not send*  
 16 *a copy of a notice described in subparagraph (A) of this paragraph to the Attorney General within a*  
 17 *reasonable time after the Attorney General requests the copy.]*

18 (d) **A covered entity or vendor that complies with regulations promulgated under the**  
 19 **Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, 110 Stat. 1936) and**  
 20 **the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5,**  
 21 **Title XIII, 123 Stat. 226), as those Acts existed on the effective date of this 2019 Act, if per-**  
 22 **sonal information that is subject to ORS 646A.600 to 646A.628 is also subject to those Acts.**

23 (10) Notwithstanding the exemptions set forth in subsection (9) of this section [*and subject to*  
 24 *subsection (1)(b) of this section, a person that owns or licenses personal information], **a person, a***

25 **covered entity or a vendor** shall provide to the Attorney General within a reasonable time at least  
 26 one copy of any notice the person, **the covered entity or the vendor** sends to consumers or to the  
 27 person's, **the covered entity's or the vendor's** primary or functional regulator in compliance with  
 28 this section or with other state or federal laws or regulations that apply to the person, **the covered**  
 29 **entity or the vendor** as a consequence of a breach of security, **if the breach of security affects**  
 30 **more than 250 consumers.**

31 (11)(a) A person's violation of a provision of ORS 646A.600 to 646A.628 is an unlawful practice  
 32 under ORS 646.607.

33 (b) **A covered entity or vendor in an action or proceeding may affirmatively defend**  
 34 **against an allegation that the covered entity or vendor has not developed, implemented and**  
 35 **maintained reasonable safeguards to protect the security, confidentiality and integrity of**  
 36 **personal information that is subject to ORS 646A.600 to 646A.628 but is not subject to an Act**  
 37 **described in subsection (9)(c) or (d) of this section by showing that, with respect to the per-**  
 38 **sonal information that is subject to ORS 646A.600 to 646A.628, the covered entity or vendor**  
 39 **developed, implemented and maintained reasonable security measures that would be required**  
 40 **for personal information subject to the applicable Act.**

41 [(b)] (c) The rights and remedies available under this section are cumulative and are in addition  
 42 to any other rights or remedies that are available under law.

43 **SECTION 4.** ORS 646A.622, as amended by section 6, chapter 10, Oregon Laws 2018, is amended  
 44 to read:

45 646A.622. (1) A [*person that owns, maintains or otherwise possesses, or has control over or access*

1 *to, data that includes personal information that the person uses in the course of the person's business,*  
2 *vocation, occupation or volunteer activities]* **covered entity and a vendor** shall develop, implement  
3 and maintain reasonable safeguards to protect the security, confidentiality and integrity of [*the*]  
4 personal information, including safeguards that protect the personal information when the [*person*]  
5 **covered entity or vendor** disposes of the personal information.

6 (2) A [*person*] **covered entity or vendor** complies with subsection (1) of this section if the  
7 [*person*] **covered entity or vendor**:

8 (a) Complies with a state or federal law that provides greater protection to personal information  
9 than the protections that this section provides.

10 (b) Complies with regulations promulgated under Title V of the Gramm-Leach-Bliley Act of 1999  
11 (15 U.S.C. 6801 to 6809) as in effect on [*June 2, 2018*] **the effective date of this 2019 Act**, if [*the*]  
12 [*person*] **personal information that is subject to ORS 646A.600 to 646A.628** is also subject to the  
13 Act.

14 (c) Complies with regulations that implement the Health Insurance Portability and Account-  
15 ability Act of 1996 (45 C.F.R. parts 160 and 164) [*as in effect on June 2, 2018,*] **and the Health In-**  
16 **formation Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5, Title XIII,**  
17 **123 Stat. 226), as those Acts were in effect on the effective date of this 2019 Act**, if [*the*]  
18 [*person*] **personal information that is subject to ORS 646A.600 to 646A.628** is also subject to [*the*]  
19 [*Act*] **those Acts**.

20 (d) Implements an information security program that includes:

21 (A) Administrative safeguards such as:

22 (i) Designating one or more employees to coordinate the security program;

23 (ii) Identifying reasonably foreseeable internal and external risks with reasonable regularity;

24 (iii) Assessing whether existing safeguards adequately control the identified risks;

25 (iv) Training and managing employees in security program practices and procedures with rea-  
26 sonable regularity;

27 (v) Selecting service providers that are capable of maintaining appropriate safeguards and  
28 practices, and requiring the service providers by contract to maintain the safeguards and practices;

29 (vi) Adjusting the security program in light of business changes, potential threats or new cir-  
30 cumstances; and

31 (vii) Reviewing user access privileges with reasonable regularity;

32 (B) Technical safeguards such as:

33 (i) Assessing risks and vulnerabilities in network and software design and taking reasonably  
34 timely action to address the risks and vulnerabilities;

35 (ii) Applying security updates and a reasonable security patch management program to software  
36 that might reasonably be at risk of or vulnerable to a breach of security;

37 (iii) Monitoring, detecting, preventing and responding to attacks or system failures; and

38 (iv) Regularly testing, monitoring and taking action to address the effectiveness of key controls,  
39 systems and procedures; and

40 (C) Physical safeguards such as:

41 (i) Assessing, in light of current technology, risks of information collection, storage, usage, re-  
42 tention, access and disposal and implementing reasonable methods to remedy or mitigate identified  
43 risks;

44 (ii) Monitoring, detecting, preventing, isolating and responding to intrusions timely and with  
45 reasonable regularity;

1 (iii) Protecting against unauthorized access to or use of personal information during or after  
2 collecting, using, storing, transporting, retaining, destroying or disposing of the personal informa-  
3 tion; and

4 (iv) Disposing of personal information, whether the *[person]* **covered entity or vendor** disposes  
5 of the personal information on or off the *[person's]* **covered entity's or vendor's** premises or  
6 property, after the *[person]* **covered entity or vendor** no longer needs the personal information for  
7 business purposes or as required by local, state or federal law by burning, pulverizing, shredding  
8 or modifying a physical record and by destroying or erasing electronic media so that the information  
9 cannot be read or reconstructed.

10 (3) A *[person]* **covered entity or vendor** complies with subsection (2)(d)(C)(iv) of this section if  
11 the *[person]* **covered entity or vendor** contracts with another person engaged in the business of  
12 record destruction to dispose of personal information in a manner that is consistent with subsection  
13 (2)(d)(C)(iv) of this section.

14 (4) **A covered entity or vendor in an action or proceeding may affirmatively defend**  
15 **against an allegation that the covered entity or vendor has not complied with subsection (1)**  
16 **of this section with respect to personal information that is subject to ORS 646A.600 to**  
17 **646A.628 but is not subject to an Act described in subsection (2)(b) or (c) of this section by**  
18 **showing that, with respect to the personal information that is subject to ORS 646A.600 to**  
19 **646A.628, the covered entity or vendor developed, implemented and maintained reasonable**  
20 **security measures that would be required for personal information subject to the applicable**  
21 **Act.**

22 [(4)] (5) Notwithstanding subsection (2) of this section, a person that is an owner of a small  
23 business as defined in ORS 285B.123 (2) complies with subsection (1) of this section if the person's  
24 information security and disposal program contains administrative, technical and physical safe-  
25 guards and disposal measures that are appropriate for the size and complexity of the small business,  
26 the nature and scope of the small business's activities, and the sensitivity of the personal informa-  
27 tion the small business collects from or about consumers.

28 **SECTION 5. The amendments to ORS 646A.600, 646A.602, 646A.604 and 646A.622 by**  
29 **sections 1 to 4 of this 2019 Act apply to covered entities or vendors that own, license, main-**  
30 **tain, store, manage, collect, process, acquire or otherwise possess personal information, or**  
31 **that have access to personal information as a consequence of a contract, on or after the**  
32 **effective date of this 2019 Act.**

33