

# Senate Bill 1551

Sponsored by Senator PROZANSKI, Representative HOLVEY; Senators BURDICK, DEMBROW, GELSER, MAN-  
NING JR, RILEY, ROBLAN, TAYLOR, Representatives GREENLICK, MARSH, NOSSE (Presession filed.)

## 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 **as introduced**.

Requires person to report breach of security that involves personal information to financial institution that issues financial access device that stores personal information and to any other person that processed financial transaction on person's behalf using account information that was subject to breach of security. Requires person to report breach of security in most expeditious manner possible but not later than 45 days after discovering or receiving notification of breach, with certain exceptions.

Prohibits person that provides or contracts with another person to provide credit monitoring services at no charge to consumer from offering other services at same time or in connection with offer to provide credit monitoring services.

Provides that consumer reporting agency may charge fee of not more than \$10 for each placement or removal of security freeze, or replacement of personal identification number or password, in excess of single placement, removal or replacement during calendar year. Provides that consumer reporting agency may ask consumer if request for security freeze is result of receiving notification of security breach, may ask consumer to identify person that sent notification and may record consumer's response.

Permits consumer reporting agency to bring action to recover from person that experienced security breach actual costs of placing security freezes that consumer reporting agency may not charge consumer.

Takes effect on 91st day following adjournment sine die.

## A BILL FOR AN ACT

1  
2 Relating to actions after a breach of security that involves personal information; creating new pro-  
3 visions; amending ORS 646A.602, 646A.604, 646A.606, 646A.608, 646A.610 and 646A.622; and pre-  
4 scribing an effective date.

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

6 **SECTION 1.** ORS 646A.602 is amended to read:

7 646A.602. As used in ORS 646A.600 to 646A.628:

8 (1) **"Account information" means evidence for establishing a relationship between a con-**  
9 **sumer and an account the consumer holds with a financial institution, examples of which**  
10 **include, but are not limited to:**

11 (a) **An account number;**

12 (b) **The consumer's full name;**

13 (c) **A credit card or debit card number;**

14 (d) **An expiration date for the consumer's financial access device;**

15 (e) **A personal identification number or other security number; and**

16 (f) **A card verification value number, an access code, a password, a card security code**  
17 **number or similar security number that would permit access to the consumer's account.**

18 [(1)(a)] (2)(a) **"Breach of security" means an unauthorized acquisition of computerized data that**  
19 **materially compromises the security, confidentiality or integrity of personal information that a per-**  
20 **son maintains.**

21 (b) **"Breach of security" does not include an inadvertent acquisition of personal information by**

**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 a person or the person's employee or agent if the personal information is not used in violation of  
 2 applicable law or in a manner that harms or poses an actual threat to the security, confidentiality  
 3 or integrity of the personal information.

4 [(2)] (3) "Consumer" means an individual resident of this state.

5 [(3)] (4) "Consumer report" means a consumer report as described in section 603(d) of the federal  
 6 Fair Credit Reporting Act (15 U.S.C. 1681a(d)), as that Act existed on [January 1, 2016] **the effective**  
 7 **date of this 2018 Act**, that a consumer reporting agency compiles and maintains.

8 [(4)] (5) "Consumer reporting agency" means a consumer reporting agency as described in sec-  
 9 tion 603(p) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(p)) as that Act existed on  
 10 [January 1, 2016] **the effective date of this 2018 Act**.

11 [(5)] (6) "Debt" means any obligation or alleged obligation arising out of a consumer transaction.

12 [(6)] (7) "Encryption" means an algorithmic process that renders data unreadable or unusable  
 13 without the use of a confidential process or key.

14 [(7)] (8) "Extension of credit" means a right to defer paying debt or a right to incur debt and  
 15 defer paying the debt, that is offered or granted primarily for personal, family or household pur-  
 16 poses.

17 (9) "Financial access device" means a credit card, debit card or a similar or related de-  
 18 vice by means of which a consumer in conducting a transaction may make a payment that  
 19 draws on an extension of credit from a financial institution to the consumer or that with-  
 20 draws funds from an account that the consumer maintains with a financial institution.

21 (10) "Financial institution" has the meaning given that term in ORS 706.008.

22 [(8)] (11) "Identity theft" has the meaning set forth in ORS 165.800.

23 [(9)] (12) "Identity theft declaration" means a completed and signed statement that documents  
 24 alleged identity theft, using [the] a form available from the Federal Trade Commission, or another  
 25 substantially similar form.

26 [(10)] (13) "Person" means an individual, private or public corporation, partnership, cooperative,  
 27 association, estate, limited liability company, organization or other entity, whether or not organized  
 28 to operate at a profit, or a public body as defined in ORS 174.109.

29 [(11)] (14)(a) "Personal information" means:

30 [(a)] (A) A consumer's first name or first initial and last name in combination with any one or  
 31 more of the following data elements, if encryption, redaction or other methods have not rendered  
 32 the data elements unusable or if the data elements are encrypted and the encryption key has been  
 33 acquired:

34 [(A)] (i) A consumer's Social Security number;

35 [(B)] (ii) A consumer's driver license number or state identification card number issued by the  
 36 Department of Transportation;

37 [(C)] (iii) A consumer's passport number or other identification number issued by the United  
 38 States;

39 [(D)] (iv) A consumer's [financial account number, credit card number or debit card number, in  
 40 combination with any required security code, access code or password that would permit access to a  
 41 consumer's financial account] **account information**;

42 [(E)] (v) Data from automatic measurements of a consumer's physical characteristics, such as  
 43 an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the  
 44 course of a financial transaction or other transaction;

45 (vi) A consumer's user name or email address in combination with the consumer's ac-

1 **count information;**

2 (vii) **Geolocation information that can disclose a consumer's identity or location;**

3 (viii) **Photographs or other images of a consumer that could reasonably identify the**  
4 **consumer;**

5 [(F)] (ix) A consumer's health insurance policy number or health insurance subscriber identifi-  
6 cation number in combination with any other unique identifier that a health insurer uses to identify  
7 the consumer; or

8 [(G)] (x) Any information about a consumer's medical history or mental or physical condition  
9 or about a health care professional's medical diagnosis or treatment of the consumer.

10 [(b)] (B) Any of the data elements or any combination of the data elements described in [*para-*  
11 *graph (a)*] **subparagraph (A)** of this [*subsection*] **paragraph** without the consumer's first name or  
12 first initial and last name if:

13 [(A)] (i) Encryption, redaction or other methods have not rendered the data element or combi-  
14 nation of data elements unusable; and

15 [(B)] (ii) The data element or combination of data elements would enable a person to commit  
16 identity theft against a consumer.

17 (C) **Account information that is ordinarily stored on a financial access device.**

18 [(c)] (b) "Personal information" does not include information in a federal, state or local govern-  
19 ment record, other than a Social Security number, that is lawfully made available to the public.

20 [(12)] (15) "Proper identification" means written information or documentation that a consumer  
21 or representative can present to another person as evidence of the consumer's or representative's  
22 identity, examples of which include:

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

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

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

27 [(13)] (16) "Protected consumer" means an individual who is:

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

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

32 [(14)] (17) "Protective record" means information that a consumer reporting agency compiles to  
33 identify a protected consumer for whom the consumer reporting agency has not prepared a consumer  
34 report.

35 [(15)] (18) "Redacted" means altered or truncated so that no more than the last four digits of  
36 a Social Security number, driver license number, state identification card number, passport number  
37 or other number issued by the United States, financial account number, credit card number or debit  
38 card number is visible or accessible.

39 [(16)] (19) "Representative" means a consumer who provides a consumer reporting agency with  
40 sufficient proof of the consumer's authority to act on a protected consumer's behalf.

41 [(17)] (20) "Security freeze" means a notice placed in a consumer report at a consumer's request  
42 or a representative's request or in a protective record at a representative's request that, subject to  
43 certain exemptions, prohibits a consumer reporting agency from releasing information in the con-  
44 sumer report or the protective record for an extension of credit, unless the consumer temporarily  
45 lifts the security freeze on the consumer's consumer report or a protected consumer or represen-

tative removes the security freeze on or deletes the protective record.

**SECTION 2.** ORS 646A.604 is amended to read:

646A.604. (1)(a) **If a person [that] owns or licenses personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities or possesses or has access to as a consequence of a transaction with a consumer and the personal information [that] was subject to a breach of security, after discovering or receiving notice of the breach of security under subsection (2) of this section, the person shall give notice of the breach of security to:**

[(a)] **(A) The consumer to whom the personal information pertains. [after the person discovers the breach of security or after the person receives notice of a breach of security under subsection (2) of this section. The person shall notify the consumer in the most expeditious manner possible, without unreasonable delay, consistent with the legitimate needs of law enforcement described in subsection (3) of this section and consistent with any measures that are necessary to determine sufficient contact information for the affected consumer, determine the scope of the breach of security and restore the reasonable integrity, security and confidentiality of the personal information.]**

[(b)] **(B) The Attorney General, either in writing or electronically, if the number of consumers to whom the person must send the notice described in [paragraph (a)] subparagraph (A) of this [subsection] paragraph exceeds 250. [The person shall disclose the breach of security to the Attorney General in the manner described in paragraph (a) of this subsection.]**

**(C) The financial institution that issued any financial access device with account information that was subject to the breach of security.**

**(D) Any other person that processed a financial transaction on the person's behalf using account information that was subject to the breach of security.**

**(b) The person shall notify a person listed in paragraph (a) of this subsection in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security, provided that:**

**(A) The notification is consistent with the legitimate needs of a law enforcement agency that are described in subsection (3) of this section; and**

**(B) The person undertakes any measures that are necessary to:**

**(i) Determine sufficient contact information for a person listed in paragraph (a) of this subsection;**

**(ii) Determine the scope of the breach of security; and**

**(iii) Restore the reasonable integrity, security and confidentiality of the personal information.**

**(2) A person that maintains or otherwise possesses personal information on behalf of, or under license of, another person shall notify the other person after discovering a breach of security.**

**(3) A person that owns or licenses personal information, or that possesses or has access to personal information as a consequence of a transaction with a consumer, may delay notifying [a] the consumer of a breach of security only if a law enforcement agency determines that a notification will impede a criminal investigation and if the law enforcement agency requests in writing that the person delay the notification.**

**(4) For purposes of this section, a person that owns or licenses personal information, or that possesses or has access to personal information as a consequence of a transaction with a consumer, may notify [a] the consumer of a breach of security:**

**(a) In writing;**

1 (b) Electronically, if the person customarily communicates with the consumer electronically or  
 2 if the notice is consistent with the provisions regarding electronic records and signatures set forth  
 3 in the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001) as that Act ex-  
 4 isted on [*January 1, 2016*] **the effective date of this 2018 Act**;

5 (c) By telephone, if the person contacts the affected consumer directly; or

6 (d) With substitute notice, if the person demonstrates that the cost of notification otherwise  
 7 would exceed \$250,000 or that the affected class of consumers exceeds 350,000, or if the person does  
 8 not have sufficient contact information to notify affected consumers. For the purposes of this para-  
 9 graph, “substitute notice” means:

10 (A) Posting the notice or a link to the notice conspicuously on the person’s website if the person  
 11 maintains a website; and

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

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

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

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

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

17 (d) Contact information for the person that owned or licensed, **or that possessed or had access**  
 18 **to as a consequence of a transaction with a consumer**, the personal information that was subject  
 19 to the breach of security;

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

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

23 (6) If a person discovers a breach of security that affects more than 1,000 consumers, the person  
 24 shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain  
 25 reports on consumers on a nationwide basis of the timing, distribution and content of the notice the  
 26 person gave to affected consumers and shall include in the notice any police report number assigned  
 27 to the breach of security. A person may not delay notifying affected consumers of a breach of se-  
 28 curity in order to notify consumer reporting agencies.

29 **(7) A person that, as a consequence of or in connection with a breach of security, pro-**  
 30 **vides or contracts with another person to provide credit monitoring services to a consumer**  
 31 **at no charge to the consumer may not at the same time as, or in connection with, the offer**  
 32 **to provide credit monitoring services:**

33 **(a) Offer, or require or permit the other person to offer, services other than credit**  
 34 **monitoring services; or**

35 **(b) Condition the person’s provision of credit monitoring services, or permit or require**  
 36 **the other person to condition the provision of credit monitoring services, on the consumer’s**  
 37 **acceptance of services other than the credit monitoring services.**

38 [(7)] (8) Notwithstanding subsection (1) of this section, a person does not need to notify con-  
 39 sumers of a breach of security if, after an appropriate investigation or after consultation with rele-  
 40 vant federal, state or local law enforcement agencies, the person reasonably determines that the  
 41 consumers whose personal information was subject to the breach of security are unlikely to suffer  
 42 harm. The person must document the determination in writing and maintain the documentation for  
 43 at least five years.

44 [(8)] (9) This section does not apply to:

45 (a) A person that complies with notification requirements or procedures for a breach of security

1 that the person's primary or functional federal regulator adopts, promulgates or issues in rules,  
 2 regulations, procedures, guidelines or guidance, if the rules, regulations, procedures, guidelines or  
 3 guidance provide greater protection to personal information and disclosure requirements at least as  
 4 thorough as the protections and disclosure requirements provided under this section.

5 (b) A person that complies with a state or federal law that provides greater protection to per-  
 6 sonal information and disclosure requirements at least as thorough as the protections and disclosure  
 7 requirements provided under this section.

8 (c) A person that is subject to and complies with regulations promulgated pursuant to Title V  
 9 of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809) as that Act existed on [*January 1,*  
 10 *2016*] **the effective date of this 2018 Act.**

11 (d)(A) Except as provided in subparagraph (B) of this paragraph, a covered entity, as defined in  
 12 45 C.F.R. 160.103, as in effect on [*January 1, 2016*] **the effective date of this 2018 Act**, that is  
 13 governed under 45 C.F.R. parts 160 and 164, as in effect on [*January 1, 2016*] **the effective date**  
 14 **of this 2018 Act**, if the covered entity sends the Attorney General a copy of the notice the covered  
 15 entity sent to consumers under [*ORS 646A.604*] **this section** or a copy of the notice that the covered  
 16 entity sent to the primary functional regulator designated for the covered entity under the Health  
 17 Insurance Portability and Availability Act of 1996, (P.L. 104-191, 110 Stat. 1936, 42 U.S.C. 300(gg),  
 18 29 U.S.C. 118 et seq., 42 U.S.C. 1320(d) et seq., 45 C.F.R. parts 160 and 164), **as in effect on the**  
 19 **effective date of this 2018 Act.**

20 (B) A covered entity is subject to the provisions of this section if the covered entity does not  
 21 send a copy of a notice described in subparagraph (A) of this paragraph to the Attorney General  
 22 within a reasonable time after the Attorney General requests the copy.

23 [(9)(a)] **(10)(a)** A person's violation of a provision of ORS 646A.600 to 646A.628 is an unlawful  
 24 practice under ORS 646.607.

25 (b) The rights and remedies available under this section are cumulative and are in addition to  
 26 any other rights or remedies that are available under law.

27 **SECTION 3.** ORS 646A.606 is amended to read:

28 646A.606. (1) A consumer may elect to place a security freeze on the consumer's consumer re-  
 29 port or, if the consumer is a representative, on a protected consumer's consumer report or protec-  
 30 tive record by sending a written request to a consumer reporting agency at an address the agency  
 31 designates to receive such requests, or a secure electronic request at a website the agency desig-  
 32 nates to receive such requests if the consumer reporting agency, at the agency's discretion, makes  
 33 a secure electronic method available.

34 (2) If the consumer or protected consumer is the victim of identity theft or has reported a theft  
 35 of personal information to a law enforcement agency, the consumer or representative may include  
 36 a copy of the police report, incident report or identity theft declaration.

37 (3)(a) The consumer or representative must provide proper identification and any **applicable** fee  
 38 authorized by ORS 646A.610.

39 (b)(A) In addition to the information and fee described in paragraph (a) of this subsection, a  
 40 representative who seeks to place a security freeze on a protected consumer's consumer report or  
 41 protective record shall provide sufficient proof of the representative's authority to act on the pro-  
 42 tected consumer's behalf.

43 (B) For purposes of subparagraph (A) of this paragraph, sufficient proof of authority consists of:

44 (i) A court order that identifies or describes the relationship between the representative and the  
 45 protected consumer;

1 (ii) A valid and lawfully executed power of attorney that permits the representative to act on  
2 the protected consumer's behalf; or

3 (iii) A written affidavit that the representative signs and has notarized in which the represen-  
4 tative expressly describes the relationship between the representative and the protected consumer  
5 and the representative's authority to act on the protected consumer's behalf.

6 (4)(a) Except as provided in ORS 646A.614, if a security freeze is in place for a consumer report,  
7 information from the consumer report may not be released without prior express authorization from  
8 the consumer.

9 (b) Information from a protective record may not be released until the protected consumer for  
10 whom the consumer reporting agency created the protective record, or a representative of the pro-  
11 tected consumer, removes the security freeze.

12 (5) This section does not prevent a consumer reporting agency from advising a third party that  
13 a security freeze is in effect with respect to the consumer report or protective record.

14 **SECTION 4.** ORS 646A.608 is amended to read:

15 646A.608. (1)(a) A consumer reporting agency shall place a security freeze on a consumer report  
16 not later than five business days after receiving from a consumer:

17 (A) The request described in ORS 646A.606 (1);

18 (B) Proper identification; and

19 (C) A fee, if applicable.

20 (b) If a consumer report does not exist for a protected consumer on behalf of whom a repre-  
21 sentative seeks to place a security freeze, a consumer reporting agency shall create a protective  
22 record after receiving from the representative the request described in ORS 646A.606 (1), proper  
23 identification for both the representative and the protected consumer and sufficient proof of au-  
24 thority, as described in ORS 646A.606 (3)(b). After creating a protective record for a protected con-  
25 sumer under this paragraph, the consumer reporting agency shall place the security freeze that the  
26 representative requested on the protected consumer's protective record.

27 (c) The protective record that the consumer reporting agency creates under paragraph (b) of this  
28 subsection does not need to contain any information other than the protected consumer's personal  
29 information, if other information for the protected consumer is not available. Except as provided in  
30 ORS 646A.614, a consumer reporting agency may not use or release to another person the informa-  
31 tion in a protective record for the purpose of assessing a protected consumer's eligibility or capacity  
32 for an extension of credit, as a basis for evaluating a protected consumer's character, reputation or  
33 personal characteristics or for other purposes that are not related to protecting the protected con-  
34 sumer from identity theft.

35 (2)(a) The consumer reporting agency shall send a written confirmation of a security freeze on  
36 a consumer's consumer report to the consumer at the last known address for the consumer shown  
37 in the consumer report that the consumer reporting agency maintains, within 10 business days after  
38 placing the security freeze and, with the confirmation, shall provide the consumer with a unique  
39 personal identification number or password or similar device the consumer must use to authorize the  
40 consumer reporting agency to release the consumer's consumer report for a specific period of time  
41 or to permanently remove the security freeze. The consumer reporting agency shall include with the  
42 written confirmation information that describes how to remove a security freeze and how to tem-  
43 porarily lift a security freeze on a consumer report, other than a consumer report for a protected  
44 consumer, in order to allow access to information from the consumer's consumer report for a period  
45 of time while the security freeze is in place.

1 (b) This subsection does not require a consumer reporting agency to provide a consumer or  
2 representative with a personal identification number or password for the consumer or representative  
3 to use to authorize the consumer reporting agency to release information from a protective record.

4 (3)(a) If a consumer wishes to allow the consumer's consumer report to be accessed for a specific  
5 period of time while a security freeze is in effect, the consumer shall contact the consumer reporting  
6 agency using a point of contact the consumer reporting agency designates, request that the security  
7 freeze be temporarily lifted and provide the following:

8 (A) Proper identification;

9 (B) The unique personal identification number or password or similar device the consumer re-  
10 porting agency provided under subsection (2) of this section; **and**

11 (C) An indication of the period of time during which the consumer report must be available to  
12 users of the consumer report[; *and*].

13 [*(D) A fee, if applicable.*]

14 (b) A protective record is not subject to a temporary lift of a security freeze.

15 (c) Except as provided in ORS 646A.612 (2)(a), a consumer report for a protected consumer is  
16 not subject to a temporary lift of a security freeze.

17 (4) A consumer reporting agency that receives a request from [*the*] a consumer to temporarily  
18 lift a security freeze on a consumer report, other than a consumer report for a protected consumer,  
19 under subsection (3) of this section shall comply with the request not later than three business days  
20 after receiving from the consumer:

21 (a) Proper identification;

22 (b) The unique personal identification number or password or similar device the consumer re-  
23 porting agency provided under subsection (2) of this section; **and**

24 (c) An indication of the period of time during which the consumer report must be available to  
25 users of the consumer report[; *and*].

26 [*(d) A fee, if applicable.*]

27 (5)(a) A security freeze for a consumer report must remain in place until the consumer requests,  
28 using a point of contact the consumer reporting agency designates, that the security freeze be re-  
29 moved. A consumer reporting agency shall remove a security freeze within three business days after  
30 receiving a request for removal from the consumer, who provides:

31 (A) Proper identification;

32 (B) The unique personal identification number or password or similar device the consumer re-  
33 porting agency provided under subsection (2) of this section; and

34 (C) A fee, if applicable.

35 (b) A security freeze for a protective record must remain in place until the protected consumer  
36 or a representative requests, using a point of contact the consumer reporting agency designates,  
37 that the security freeze be removed or that the protective record be deleted. The consumer reporting  
38 agency does not have an affirmative duty to notify the protected consumer or the representative  
39 that a security freeze is in place or to remove the security freeze or delete the protective record  
40 once the protected consumer is no longer a protected consumer. A protected consumer or a repre-  
41 sentative has the affirmative duty to request that the consumer reporting agency remove the secu-  
42 rity freeze or delete the protective record. A consumer reporting agency shall remove a security  
43 freeze or delete a protective record within 30 business days after receiving a request for removal  
44 or deletion from the protected consumer or a representative, who provides:

45 (A) Proper identification;

1 (B) Sufficient proof of authority, as described in ORS 646A.606 (3)(b), if the representative seeks  
2 to remove the security freeze or delete the protective record;

3 (C) Proof that the representative's authority to act on the protected consumer's behalf is no  
4 longer valid or applicable, if the protected consumer seeks to remove the security freeze or delete  
5 the protective record; and

6 (D) A fee, if applicable.

7 **SECTION 5.** ORS 646A.610 is amended to read:

8 646A.610. (1) A consumer reporting agency may not charge a fee to a consumer or a protected  
9 consumer who is the victim of identity theft or to a consumer who has reported, or a protected  
10 consumer for whom a representative has reported, to a law enforcement agency the theft of personal  
11 information, provided the consumer or the representative has submitted to the consumer reporting  
12 agency a copy of a valid police report, incident report or identity theft declaration.

13 *[(2)(a) A consumer reporting agency may charge a reasonable fee of not more than \$10 to a con-  
14 sumer, other than a consumer described in subsection (1) of this section, for each placement of a secu-  
15 rity freeze, temporary lift of the security freeze, removal of the security freeze or replacing a lost  
16 personal identification number or password previously provided to the consumer.]*

17 *[(b)(A) Except as provided in subsection (1) of this section and in subparagraph (B) of this para-  
18 graph, a consumer reporting agency may charge a reasonable fee of not more than \$10 to place or re-  
19 move a security freeze for a protected consumer's consumer report or protective record or to create or  
20 delete a protective record for a protected consumer.]*

21 **(2)(a) A consumer reporting agency may charge a consumer, other than a consumer de-  
22 scribed in subsection (1) of this section, a fee of not more than \$10 for each placement or  
23 removal of a security freeze, or replacement of a personal identification number or password,  
24 in excess of a single placement, removal or replacement during the calendar year.**

25 **(b)(A) Except as provided in subparagraph (B) of this paragraph, a consumer reporting  
26 agency may charge a consumer a fee of not more than \$10 for each creation or deletion of  
27 a protective record, or placement or removal of a security freeze for a protected consumer,  
28 in excess of a single creation, deletion, placement or removal during the calendar year.**

29 (B) A consumer reporting agency may not charge a fee to place or remove a security freeze on  
30 an existing consumer report or protective record for a protected consumer who is under 16 years  
31 of age at the time a representative requests the consumer reporting agency to place or remove the  
32 security freeze.

33 **(3) A consumer reporting agency may ask a consumer if the consumer is requesting a  
34 security freeze as a result of receiving notification of a breach of security and may ask the  
35 consumer to identify the person that sent the notification. The consumer reporting agency  
36 may record the consumer's response to a question under this subsection after notifying the  
37 consumer that the consumer reporting agency will record the consumer's response.**

38 **(4) A consumer reporting agency may bring an action to recover the consumer reporting  
39 agency's actual costs of placing security freezes for consumers as a direct result of a breach  
40 of security. The consumer reporting agency may bring the action only against a single de-  
41 fendant, which must be a person that owns, licenses, possesses or has access to, as a con-  
42 sequence of a transaction with a consumer, the personal information involved in the breach  
43 of security. The amount of the consumer reporting agency's recovery may not exceed \$10 for  
44 each security freeze the consumer reporting agency placed as a direct result of the breach  
45 of security and for which the consumer reporting agency could not charge a consumer under**

1 **subsection (2) of this section. A consumer reporting agency may not recover consequential**  
 2 **or punitive damages or attorney fees and costs in the action.**

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

4 646A.622. (1) A person that owns, maintains or otherwise possesses data that includes a  
 5 consumer's personal information that the person uses in the course of the person's business, voca-  
 6 tion, occupation or volunteer activities shall develop, implement and maintain reasonable safeguards  
 7 to protect the security, confidentiality and integrity of the personal information, including safe-  
 8 guards that protect the personal information when the person disposes of the personal information.

9 (2) A person complies with subsection (1) of this section if the person:

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

12 (b) Complies with regulations promulgated under Title V of the Gramm-Leach-Bliley Act of 1999  
 13 (15 U.S.C. 6801 to 6809) as in effect on [*January 1, 2016*] **the effective date of this 2018 Act**, if the  
 14 person is subject to the Act.

15 (c) Complies with regulations that implement the Health Insurance Portability and Account-  
 16 ability Act of 1996 (45 C.F.R. parts 160 and 164) as in effect on [*January 1, 2016*] **the effective date**  
 17 **of this 2018 Act**, if the person is subject to the Act.

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

19 (A) Administrative safeguards such as:

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

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

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

23 (iv) Training and managing employees in security program practices and procedures **with rea-**  
 24 **sonable regularity**;

25 (v) Selecting service providers that are capable of maintaining appropriate safeguards **and ad-**  
 26 **hering to procedures and protocols to which the person and the service provider agree**, and  
 27 requiring the service providers by contract to maintain the safeguards, **procedures and protocols**;  
 28 [*and*]

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

31 **(vii) Training employees to identify potential threats and assess the business impact of**  
 32 **the potential threats**;

33 **(viii) Monitoring, verifying, logging and disseminating information about security updates**  
 34 **and upgrades to software that might be at risk of or vulnerable to a breach of security**; and

35 **(ix) Reviewing user access policies with reasonable regularity**;

36 (B) Technical safeguards such as:

37 (i) Assessing risks **and vulnerabilities** in network and software design **and in information**  
 38 **collection, processing, transmission, retention, access, storage and disposal and taking timely**  
 39 **action to address the risks and vulnerabilities with reasonable regularity**;

40 (ii) [*Assessing risks in information processing, transmission and storage*] **Applying security up-**  
 41 **dates and upgrades to software that might be at risk of or vulnerable to a breach of**  
 42 **security**;

43 (iii) **Monitoring**, detecting, preventing and responding to attacks or system failures; [*and*]

44 (iv) Testing and monitoring regularly the effectiveness of key controls, systems and procedures  
 45 **and taking action to reduce or eliminate weaknesses, deficiencies and risks in the controls**,

1 **systems and procedures; and**

2 **(v) Isolating and segregating personal information from other information and ensuring**  
 3 **that only authorized individuals have access to the personal information; and**

4 (C) Physical safeguards such as:

5 [(i) *Assessing risks of information storage and disposal;*]

6 [(ii)] (i) **Monitoring**, detecting, preventing, **isolating** and responding to intrusions **timely and**  
 7 **with reasonable regularity;**

8 [(iii)] (ii) Protecting against unauthorized access to or use of personal information during or  
 9 after collecting, **using**, transporting, **retaining**, destroying or disposing of the personal information;  
 10 and

11 [(iv)] (iii) Disposing of personal information, **whether on or off of the person's premises or**  
 12 **property**, after the person no longer needs the personal information for business purposes or as  
 13 required by local, state or federal law by burning, pulverizing, shredding or modifying a physical  
 14 record and by destroying or erasing electronic media so that the information cannot be read or re-  
 15 constructed.

16 (3) A person complies with subsection [(2)(d)(C)(iv)] **(2)(d)(C)(iii)** of this section if the person  
 17 contracts with another person engaged in the business of record destruction to dispose of personal  
 18 information in a manner that is consistent with subsection [(2)(d)(C)(iv)] **(2)(d)(C)(iii)** of this section.

19 (4) Notwithstanding subsection (2) of this section, a person that is an owner of a small business  
 20 as defined in ORS 285B.123 (2) complies with subsection (1) of this section if the person's information  
 21 security and disposal program contains administrative, technical and physical safeguards and dis-  
 22 posal measures that are appropriate for the size and complexity of the small business, the nature  
 23 and scope of the small business's activities, and the sensitivity of the personal information the small  
 24 business collects from or about consumers.

25 **SECTION 7. The amendments to ORS 646A.602, 646A.604, 646A.606, 646A.608, 646A.610 and**  
 26 **646A.622 by sections 1 to 6 of this 2018 Act apply to contracts into which a person enters**  
 27 **with another person on or after the effective date of this 2018 Act.**

28 **SECTION 8. This 2018 Act takes effect on the 91st day after the date on which the 2018**  
 29 **regular session of the Seventy-ninth Legislative Assembly adjourns sine die.**

30