

DRAFT

SUMMARY

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 infor-
3 mation; creating new provisions; amending ORS 646A.602, 646A.604,
4 646A.606, 646A.608, 646A.610 and 646A.622; and prescribing an effective
5 date.

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

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

1 646A.602. As used in ORS 646A.600 to 646A.628:

2 **(1) “Account information” means evidence for establishing a re-**
3 **lationship between a consumer and an account the consumer holds**
4 **with a financial institution, examples of which include, but are not**
5 **limited to:**

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

7 **(b) The consumer’s full name;**

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

9 **(d) An expiration date for the consumer’s financial access device;**

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

11 **(f) A card verification value number, an access code, a password, a**
12 **card security code number or similar security number that would**
13 **permit access to the consumer’s account.**

14 [(1)(a)] **(2)(a)** “Breach of security” means an unauthorized acquisition of
15 computerized data that materially compromises the security, confidentiality
16 or integrity of personal information that a person maintains.

17 (b) “Breach of security” does not include an inadvertent acquisition of
18 personal information by a person or the person’s employee or agent if the
19 personal information is not used in violation of applicable law or in a man-
20 ner that harms or poses an actual threat to the security, confidentiality or
21 integrity of the personal information.

22 [(2)] **(3)** “Consumer” means an individual resident of this state.

23 [(3)] **(4)** “Consumer report” means a consumer report as described in sec-
24 tion 603(d) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)), as
25 that Act existed on [January 1, 2016] **the effective date of this 2018 Act,**
26 that a consumer reporting agency compiles and maintains.

27 [(4)] **(5)** “Consumer reporting agency” means a consumer reporting agency
28 as described in section 603(p) of the federal Fair Credit Reporting Act (15
29 U.S.C. 1681a(p)) as that Act existed on [January 1, 2016] **the effective date**
30 **of this 2018 Act.**

31 [(5)] **(6)** “Debt” means any obligation or alleged obligation arising out of

1 a consumer transaction.

2 [(6)] (7) “Encryption” means an algorithmic process that renders data
3 unreadable or unusable without the use of a confidential process or key.

4 [(7)] (8) “Extension of credit” means a right to defer paying debt or a
5 right to incur debt and defer paying the debt, that is offered or granted pri-
6 marily for personal, family or household purposes.

7 (9) “Financial access device” means a credit card, debit card or a
8 similar or related device by means of which a consumer in conducting
9 a transaction may make a payment that draws on an extension of
10 credit from a financial institution to the consumer or that withdraws
11 funds from an account that the consumer maintains with a financial
12 institution.

13 (10) “Financial institution” has the meaning given that term in ORS
14 706.008.

15 [(8)] (11) “Identity theft” has the meaning set forth in ORS 165.800.

16 [(9)] (12) “Identity theft declaration” means a completed and signed
17 statement that documents alleged identity theft, using [*the*] a form available
18 from the Federal Trade Commission, or another substantially similar form.

19 [(10)] (13) “Person” means an individual, private or public corporation,
20 partnership, cooperative, association, estate, limited liability company, or-
21 ganization or other entity, whether or not organized to operate at a profit,
22 or a public body as defined in ORS 174.109.

23 [(11)] (14)(a) “Personal information” means:

24 [(a)] (A) A consumer’s first name or first initial and last name in combi-
25 nation with any one or more of the following data elements, if encryption,
26 redaction or other methods have not rendered the data elements unusable
27 or if the data elements are encrypted and the encryption key has been ac-
28 quired:

29 [(A)] (i) A consumer’s Social Security number;

30 [(B)] (ii) A consumer’s driver license number or state identification card
31 number issued by the Department of Transportation;

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

3 [(D)] (iv) A consumer's [*financial account number, credit card number or*
4 *debit card number, in combination with any required security code, access code*
5 *or password that would permit access to a consumer's financial account*] **ac-**
6 **count information;**

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

11 (vi) **A consumer's user name or email address in combination with**
12 **the consumer's account information;**

13 (vii) **Geolocation information that can disclose a consumer's iden-**
14 **tity or location;**

15 (viii) **Photographs or other images of a consumer that could rea-**
16 **sonably identify the consumer;**

17 [(F)] (ix) A consumer's health insurance policy number or health insur-
18 ance subscriber identification number in combination with any other unique
19 identifier that a health insurer uses to identify the consumer; or

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

23 [(b)] (B) Any of the data elements or any combination of the data ele-
24 ments described in [*paragraph (a)*] **subparagraph (A)** of this [*subsection*]
25 **paragraph** without the consumer's first name or first initial and last name
26 if:

27 [(A)] (i) Encryption, redaction or other methods have not rendered the
28 data element or combination of data elements unusable; and

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

31 (C) **Account information that is ordinarily stored on a financial**

1 **access device.**

2 [(c)] (b) “Personal information” does not include information in a federal,
3 state or local government record, other than a Social Security number, that
4 is lawfully made available to the public.

5 [(12)] (15) “Proper identification” means written information or doc-
6 umentation that a consumer or representative can present to another person
7 as evidence of the consumer’s or representative’s identity, examples of which
8 include:

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

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

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

14 [(13)] (16) “Protected consumer” means an individual who is:

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

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

19 [(14)] (17) “Protective record” means information that a consumer re-
20 porting agency compiles to identify a protected consumer for whom the con-
21 sumer reporting agency has not prepared a consumer report.

22 [(15)] (18) “Redacted” means altered or truncated so that no more than
23 the last four digits of a Social Security number, driver license number, state
24 identification card number, passport number or other number issued by the
25 United States, financial account number, credit card number or debit card
26 number is visible or accessible.

27 [(16)] (19) “Representative” means a consumer who provides a consumer
28 reporting agency with sufficient proof of the consumer’s authority to act on
29 a protected consumer’s behalf.

30 [(17)] (20) “Security freeze” means a notice placed in a consumer report
31 at a consumer’s request or a representative’s request or in a protective re-

1 cord at a representative's request that, subject to certain exemptions, pro-
 2 hibits a consumer reporting agency from releasing information in the
 3 consumer report or the protective record for an extension of credit, unless
 4 the consumer temporarily lifts the security freeze on the consumer's con-
 5 sumer report or a protected consumer or representative removes the security
 6 freeze on or deletes the protective record.

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

8 646A.604. (1)(a) **If** a person [*that*] owns or licenses personal information
 9 that the person uses in the course of the person's business, vocation, occu-
 10 pation or volunteer activities **or possesses or has access to as a conse-**
 11 **quence of a transaction with a consumer and the personal information**
 12 [*that*] was subject to a breach of security, **after discovering or receiving**
 13 **notice of the breach of security under subsection (2) of this section,**
 14 **the person** shall give notice of the breach of security to:

15 [(a)] (A) The consumer to whom the personal information pertains. [*after*
 16 *the person discovers the breach of security or after the person receives notice*
 17 *of a breach of security under subsection (2) of this section. The person shall*
 18 *notify the consumer in the most expeditious manner possible, without unrea-*
 19 *sonable delay, consistent with the legitimate needs of law enforcement de-*
 20 *scribed in subsection (3) of this section and consistent with any measures that*
 21 *are necessary to determine sufficient contact information for the affected con-*
 22 *sumer, determine the scope of the breach of security and restore the reasonable*
 23 *integrity, security and confidentiality of the personal information.*]

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

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

31 (D) **Any other person that processed a financial transaction on the**

1 **person's behalf using account information that was subject to the**
2 **breach of security.**

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

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

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

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

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

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

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

19 (3) A person that owns or licenses personal information, **or that pos-**
20 **sesses or has access to personal information as a consequence of a**
21 **transaction with a consumer**, may delay notifying [a] **the** consumer of a
22 breach of security only if a law enforcement agency determines that a no-
23 tification will impede a criminal investigation and if the law enforcement
24 agency requests in writing that the person delay the notification.

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

29 (a) In writing;

30 (b) Electronically, if the person customarily communicates with the con-
31 sumer electronically or if the notice is consistent with the provisions re-

1 guarding electronic records and signatures set forth in the Electronic
2 Signatures in Global and National Commerce Act (15 U.S.C. 7001) as that
3 Act existed on [*January 1, 2016*] **the effective date of this 2018 Act**;

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

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

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

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

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

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

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

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

19 (d) Contact information for the person that owned or licensed, **or that**
20 **possessed or had access to as a consequence of a transaction with a**
21 **consumer**, the personal information that was subject to the breach of se-
22 curity;

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

24 (f) Advice to the consumer to report suspected identity theft to law
25 enforcement, including the Attorney General and the Federal Trade Com-
26 mission.

27 (6) If a person discovers a breach of security that affects more than 1,000
28 consumers, the person shall notify, without unreasonable delay, all consumer
29 reporting agencies that compile and maintain reports on consumers on a
30 nationwide basis of the timing, distribution and content of the notice the
31 person gave to affected consumers and shall include in the notice any police

1 report number assigned to the breach of security. A person may not delay
2 notifying affected consumers of a breach of security in order to notify con-
3 sumer reporting agencies.

4 **(7) A person that, as a consequence of or in connection with a**
5 **breach of security, provides or contracts with another person to pro-**
6 **vide credit monitoring services to a consumer at no charge to the**
7 **consumer may not at the same time as, or in connection with, the**
8 **offer to provide credit monitoring services:**

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

11 **(b) Condition the person's provision of credit monitoring services,**
12 **or permit or require the other person to condition the provision of**
13 **credit monitoring services, on the consumer's acceptance of services**
14 **other than the credit monitoring services.**

15 [(7)] **(8)** Notwithstanding subsection (1) of this section, a person does not
16 need to notify consumers of a breach of security if, after an appropriate in-
17 vestigation or after consultation with relevant federal, state or local law
18 enforcement agencies, the person reasonably determines that the consumers
19 whose personal information was subject to the breach of security are un-
20 likely to suffer harm. The person must document the determination in writ-
21 ing and maintain the documentation for at least five years.

22 [(8)] **(9)** This section does not apply to:

23 (a) A person that complies with notification requirements or procedures
24 for a breach of security that the person's primary or functional federal reg-
25 ulator adopts, promulgates or issues in rules, regulations, procedures,
26 guidelines or guidance, if the rules, regulations, procedures, guidelines or
27 guidance provide greater protection to personal information and disclosure
28 requirements at least as thorough as the protections and disclosure require-
29 ments provided under this section.

30 (b) A person that complies with a state or federal law that provides
31 greater protection to personal information and disclosure requirements at

1 least as thorough as the protections and disclosure requirements provided
2 under this section.

3 (c) A person that is subject to and complies with regulations promulgated
4 pursuant to Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801
5 to 6809) as that Act existed on [*January 1, 2016*] **the effective date of this**
6 **2018 Act**.

7 (d)(A) Except as provided in subparagraph (B) of this paragraph, a cov-
8 ered entity, as defined in 45 C.F.R. 160.103, as in effect on [*January 1, 2016*]
9 **the effective date of this 2018 Act**, that is governed under 45 C.F.R. parts
10 160 and 164, as in effect on [*January 1, 2016*] **the effective date of this 2018**
11 **Act**, if the covered entity sends the Attorney General a copy of the notice
12 the covered entity sent to consumers under [*ORS 646A.604*] **this section** or
13 a copy of the notice that the covered entity sent to the primary functional
14 regulator designated for the covered entity under the Health Insurance Por-
15 tability and Availability Act of 1996, (P.L. 104-191, 110 Stat. 1936, 42 U.S.C.
16 300(gg), 29 U.S.C. 118 et seq., 42 U.S.C. 1320(d) et seq., 45 C.F.R. parts 160
17 and 164), **as in effect on the effective date of this 2018 Act**.

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

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

24 (b) The rights and remedies available under this section are cumulative
25 and are in addition to any other rights or remedies that are available under
26 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
29 consumer's consumer report or, if the consumer is a representative, on a
30 protected consumer's consumer report or protective record by sending a
31 written request to a consumer reporting agency at an address the agency

1 designates to receive such requests, or a secure electronic request at a
2 website the agency designates to receive such requests if the consumer re-
3 porting agency, at the agency's discretion, makes a secure electronic method
4 available.

5 (2) If the consumer or protected consumer is the victim of identity theft
6 or has reported a theft of personal information to a law enforcement agency,
7 the consumer or representative may include a copy of the police report, in-
8 cident report or identity theft declaration.

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

11 (b)(A) In addition to the information and fee described in paragraph (a)
12 of this subsection, a representative who seeks to place a security freeze on
13 a protected consumer's consumer report or protective record shall provide
14 sufficient proof of the representative's authority to act on the protected
15 consumer's behalf.

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

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

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

22 (iii) A written affidavit that the representative signs and has notarized
23 in which the representative expressly describes the relationship between the
24 representative and the protected consumer and the representative's authority
25 to act on the protected consumer's behalf.

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

29 (b) Information from a protective record may not be released until the
30 protected consumer for whom the consumer reporting agency created the
31 protective record, or a representative of the protected consumer, removes the

1 security freeze.

2 (5) This section does not prevent a consumer reporting agency from ad-
3 vising a third party that a security freeze is in effect with respect to the
4 consumer report or protective record.

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

6 646A.608. (1)(a) A consumer reporting agency shall place a security freeze
7 on a consumer report not later than five business days after receiving from
8 a consumer:

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

10 (B) Proper identification; and

11 (C) A fee, if applicable.

12 (b) If a consumer report does not exist for a protected consumer on behalf
13 of whom a representative seeks to place a security freeze, a consumer re-
14 porting agency shall create a protective record after receiving from the rep-
15 resentative the request described in ORS 646A.606 (1), proper identification
16 for both the representative and the protected consumer and sufficient proof
17 of authority, as described in ORS 646A.606 (3)(b). After creating a protective
18 record for a protected consumer under this paragraph, the consumer report-
19 ing agency shall place the security freeze that the representative requested
20 on the protected consumer's protective record.

21 (c) The protective record that the consumer reporting agency creates un-
22 der paragraph (b) of this subsection does not need to contain any information
23 other than the protected consumer's personal information, if other informa-
24 tion for the protected consumer is not available. Except as provided in ORS
25 646A.614, a consumer reporting agency may not use or release to another
26 person the information in a protective record for the purpose of assessing a
27 protected consumer's eligibility or capacity for an extension of credit, as a
28 basis for evaluating a protected consumer's character, reputation or personal
29 characteristics or for other purposes that are not related to protecting the
30 protected consumer from identity theft.

31 (2)(a) The consumer reporting agency shall send a written confirmation

1 of a security freeze on a consumer's consumer report to the consumer at the
2 last known address for the consumer shown in the consumer report that the
3 consumer reporting agency maintains, within 10 business days after placing
4 the security freeze and, with the confirmation, shall provide the consumer
5 with a unique personal identification number or password or similar device
6 the consumer must use to authorize the consumer reporting agency to release
7 the consumer's consumer report for a specific period of time or to perma-
8 nently remove the security freeze. The consumer reporting agency shall in-
9 clude with the written confirmation information that describes how to
10 remove a security freeze and how to temporarily lift a security freeze on a
11 consumer report, other than a consumer report for a protected consumer, in
12 order to allow access to information from the consumer's consumer report
13 for a period of time while the security freeze is in place.

14 (b) This subsection does not require a consumer reporting agency to pro-
15 vide a consumer or representative with a personal identification number or
16 password for the consumer or representative to use to authorize the con-
17 sumer reporting agency to release information from a protective record.

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

23 (A) Proper identification;

24 (B) The unique personal identification number or password or similar
25 device the consumer reporting agency provided under subsection (2) of this
26 section; **and**

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

29 [(D) A fee, if applicable.]

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

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

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

8 (a) Proper identification;

9 (b) The unique personal identification number or password or similar de-
10 vice the consumer reporting agency provided under subsection (2) of this
11 section; **and**

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

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

15 (5)(a) A security freeze for a consumer report must remain in place until
16 the consumer requests, using a point of contact the consumer reporting
17 agency designates, that the security freeze be removed. A consumer reporting
18 agency shall remove a security freeze within three business days after re-
19 ceiving a request for removal from the consumer, who provides:

20 (A) Proper identification;

21 (B) The unique personal identification number or password or similar
22 device the consumer reporting agency provided under subsection (2) of this
23 section; and

24 (C) A fee, if applicable.

25 (b) A security freeze for a protective record must remain in place until
26 the protected consumer or a representative requests, using a point of contact
27 the consumer reporting agency designates, that the security freeze be re-
28 moved or that the protective record be deleted. The consumer reporting
29 agency does not have an affirmative duty to notify the protected consumer
30 or the representative that a security freeze is in place or to remove the se-
31 curity freeze or delete the protective record once the protected consumer is

1 no longer a protected consumer. A protected consumer or a representative
2 has the affirmative duty to request that the consumer reporting agency re-
3 move the security freeze or delete the protective record. A consumer report-
4 ing agency shall remove a security freeze or delete a protective record within
5 30 business days after receiving a request for removal or deletion from the
6 protected consumer or a representative, who provides:

7 (A) Proper identification;

8 (B) Sufficient proof of authority, as described in ORS 646A.606 (3)(b), if
9 the representative seeks to remove the security freeze or delete the protec-
10 tive record;

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

14 (D) A fee, if applicable.

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

16 646A.610. (1) A consumer reporting agency may not charge a fee to a
17 consumer or a protected consumer who is the victim of identity theft or to
18 a consumer who has reported, or a protected consumer for whom a repre-
19 sentative has reported, to a law enforcement agency the theft of personal
20 information, provided the consumer or the representative has submitted to
21 the consumer reporting agency a copy of a valid police report, incident re-
22 port or identity theft declaration.

23 *[(2)(a) A consumer reporting agency may charge a reasonable fee of not*
24 *more than \$10 to a consumer, other than a consumer described in subsection*
25 *(1) of this section, for each placement of a security freeze, temporary lift of the*
26 *security freeze, removal of the security freeze or replacing a lost personal*
27 *identification number or password previously provided to the consumer.]*

28 *[(b)(A) Except as provided in subsection (1) of this section and in subpar-*
29 *agraph (B) of this paragraph, a consumer reporting agency may charge a rea-*
30 *sonable fee of not more than \$10 to place or remove a security freeze for a*
31 *protected consumer's consumer report or protective record or to create or delete*

1 *a protective record for a protected consumer.]*

2 **(2)(a) A consumer reporting agency may charge a consumer, other**
3 **than a consumer described in subsection (1) of this section, a fee of**
4 **not more than \$10 for each placement or removal of a security freeze,**
5 **or replacement of a personal identification number or password, in**
6 **excess of a single placement, removal or replacement during the cal-**
7 **endar year.**

8 **(b)(A) Except as provided in subparagraph (B) of this paragraph, a**
9 **consumer reporting agency may charge a consumer a fee of not more**
10 **than \$10 for each creation or deletion of a protective record, or place-**
11 **ment or removal of a security freeze for a protected consumer, in ex-**
12 **cess of a single creation, deletion, placement or removal during the**
13 **calendar year.**

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

19 **(3) A consumer reporting agency may ask a consumer if the con-**
20 **sumer is requesting a security freeze as a result of receiving notifica-**
21 **tion of a breach of security and may ask the consumer to identify the**
22 **person that sent the notification. The consumer reporting agency may**
23 **record the consumer's response to a question under this subsection**
24 **after notifying the consumer that the consumer reporting agency will**
25 **record the consumer's response.**

26 **(4) A consumer reporting agency may bring an action to recover the**
27 **consumer reporting agency's actual costs of placing security freezes**
28 **for consumers as a direct result of a breach of security. The consumer**
29 **reporting agency may bring the action only against a single defendant,**
30 **which must be a person that owns, licenses, possesses or has access**
31 **to, as a consequence of a transaction with a consumer, the personal**

1 **information involved in the breach of security. The amount of the**
2 **consumer reporting agency's recovery may not exceed \$10 for each**
3 **security freeze the consumer reporting agency placed as a direct result**
4 **of the breach of security and for which the consumer reporting agency**
5 **could not charge a consumer under subsection (2) of this section. A**
6 **consumer reporting agency may not recover consequential or punitive**
7 **damages or attorney fees and costs in the action.**

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

9 646A.622. (1) A person that owns, maintains or otherwise possesses data
10 that includes a consumer's personal information that the person uses in the
11 course of the person's business, vocation, occupation or volunteer activities
12 shall develop, implement and maintain reasonable safeguards to protect the
13 security, confidentiality and integrity of the personal information, including
14 safeguards that protect the personal information when the person disposes
15 of the personal information.

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

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

19 (b) Complies with regulations promulgated under Title V of the Gramm-
20 Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809) as in effect on [*January 1,*
21 *2016*] **the effective date of this 2018 Act**, if the person is subject to the
22 Act.

23 (c) Complies with regulations that implement the Health Insurance Por-
24 tability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164) as in
25 effect on [*January 1, 2016*] **the effective date of this 2018 Act**, if the person
26 is subject to the Act.

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

28 (A) Administrative safeguards such as:

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

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

1 (iii) Assessing whether existing safeguards adequately control the identi-
2 fied risks;

3 (iv) Training and managing employees in security program practices and
4 procedures **with reasonable regularity**;

5 (v) Selecting service providers that are capable of maintaining appropri-
6 ate safeguards **and adhering to procedures and protocols to which the**
7 **person and the service provider agree**, and requiring the service providers
8 by contract to maintain the safeguards, **procedures and protocols**; [*and*]

9 (vi) Adjusting the security program in light of business changes, **poten-**
10 **tial threats** or new circumstances;

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

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

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

17 (B) Technical safeguards such as:

18 (i) Assessing risks **and vulnerabilities** in network and software design
19 **and in information collection, processing, transmission, retention, ac-**
20 **cess, storage and disposal and taking timely action to address the risks**
21 **and vulnerabilities with reasonable regularity**;

22 (ii) [*Assessing risks in information processing, transmission and storage*]
23 **Applying security updates and upgrades to software that might be at**
24 **risk of or vulnerable to a breach of security**;

25 (iii) **Monitoring**, detecting, preventing and responding to attacks or sys-
26 tem failures; [*and*]

27 (iv) Testing and monitoring regularly the effectiveness of key controls,
28 systems and procedures **and taking action to reduce or eliminate weak-**
29 **nesses, deficiencies and risks in the controls, systems and procedures**;
30 and

31 **(v) Isolating and segregating personal information from other in-**

1 **formation and ensuring that only authorized individuals have access**
2 **to the personal information; and**

3 (C) Physical safeguards such as:

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

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

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

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

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

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

28 **SECTION 7. The amendments to ORS 646A.602, 646A.604, 646A.606,**
29 **646A.608, 646A.610 and 646A.622 by sections 1 to 6 of this 2018 Act apply**
30 **to contracts into which a person enters with another person on or af-**
31 **ter the effective date of this 2018 Act.**

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

4
