CHAPTER 10

AN ACT SB 1551

Relating to actions after a breach of security that involves personal information; creating new provisions; amending ORS 646A.602, 646A.604, 646A.606, 646A.608, 646A.610 and 646A.622; and prescribing an effective date.

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

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

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

(1)(a) "Breach of security" means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains.

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

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

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

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

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

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

(7) "Extension of credit" means a right to defer paying debt or a right to incur debt and defer paying the debt, that is offered or granted primarily for personal, family or household purposes.

(8) "Identity theft" has the meaning set forth in ORS 165.800.

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

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

(11)**(a)** "Personal information" means:

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

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

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

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

[*(D)*] **(iv)** A consumer's financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account**, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account**;

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

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

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

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

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

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

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

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

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

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

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

(13) "Protected consumer" means an individual who is:

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

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

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

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

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

(17) "Security freeze" means a notice placed in a consumer report at a consumer's request or a representative's request or in a protective record at a representative's request that, subject to certain exemptions, prohibits a consumer reporting agency from releasing information in the consumer report or the protective record for an extension of credit, unless the consumer temporarily lifts the security freeze on the consumer's consumer report or a protected consumer or representative removes the security freeze on or deletes the protective record.

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

646A.604. (1) **If** a person [*that*] owns**,** [*or*] licenses **or otherwise possesses** personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities and that was subject to a breach of security **or if the person received notice of a breach of security from another person that maintains or otherwise possesses personal information on the person's behalf, the person** shall give notice of the breach of security to:

(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) 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) of this subsection exceeds 250. [*The person shall disclose the breach of security to the Attorney General in the manner described in paragraph (a) of this subsection.*]

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

(3)(a) Except as provided in paragraph (b) of this subsection, a person that must give notice of a breach of security under this section shall give the notice 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. In providing the notice, the person shall undertake reasonable measures that are necessary to:

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

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

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

[*(3)*] **(b)** A person that [*owns or licenses personal information*] **must give notice of a breach of security under this section** may delay [*notifying a consumer of a breach of security*] **giving the notice** 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 may notify a consumer of a breach of security:*]

(4) A person that must give notice under this section to a consumer may notify the consumer of a breach of security:

(a) In writing;

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

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

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

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

(B) Notifying major statewide television and newspaper media.

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

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

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

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

[*(d) Contact information for the person that owned or licensed the personal information that was subject to the breach of security;*]

(d) Contact information for the person that gave the notice;

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

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

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

(7)(a) If a person must notify a consumer of a breach of security under this section, and in connection with the notification the person offers to provide credit monitoring services or identity theft prevention and mitigation services without charge to the consumer, the person may not condition the person's provision of the services on the consumer's providing the person with a credit or debit card number or on the consumer's acceptance of any other service the person offers to provide for a fee.

(b) If a person offers additional credit monitoring services or identity theft prevention and mitigation services for a fee to a consumer under the circumstances described in paragraph (a) of this subsection, the person must separately, distinctly, clearly and conspicuously disclose in the offer for the additional credit monitoring services or identity theft prevention and mitigation services that the person will charge the consumer a fee.

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

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

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

(a) A person that complies with notification requirements or procedures for a breach of security that the person's primary or functional federal regulator adopts, promulgates or issues in rules, regulations, procedures, guidelines or guidance, if the rules, regulations, procedures, guidelines or guidance provides greater protection to personal information and disclosure requirements at least as thorough as the protections and disclosure requirements provided under this section.

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

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

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

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

(10) Notwithstanding the exemptions set forth in subsection (9) of this section and subject to subsection (1)(b) of this section, a person that owns or licenses personal information shall provide to the Attorney General within a reasonable time at least one copy of any notice the person sends to consumers or to the person's primary or functional regulator in compliance with this section or with other state or federal laws or regulations that apply to the person as a consequence of a breach of security.

[*(9)(a)*] **(11)(a)** A person's violation of a provision of ORS 646A.600 to 646A.628 is an unlawful practice under ORS 646.607.

(b) The rights and remedies available under this section are cumulative and are in addition to any

other rights or remedies that are available under law.

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

646A.606. (1) A consumer may elect to place a security freeze on the consumer's consumer report or, if the consumer is a representative, on a protected consumer's consumer report or protective record by sending a written request to a consumer reporting agency at an address the agency designates to receive such requests, or a secure electronic request at a website the agency designates to receive such requests if the consumer reporting agency, at the agency's discretion, makes a secure electronic method available.

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

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

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

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

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

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

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

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

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

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

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

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

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

(B) Proper identification**.**[*; and*]

[*(C) A fee, if applicable.*]

(b) If a consumer report does not exist for a protected consumer on behalf of whom a representative seeks to place a security freeze, a consumer reporting agency shall create a protective record after receiving from the representative the request described in ORS 646A.606 (1), proper identification for both the representative and the protected consumer and sufficient proof of authority, as described in ORS 646A.606 (3)(b). After creating a protective record for a protected consumer under this paragraph, the consumer reporting agency shall place the security freeze that the representative requested on the protected consumer's protective record.

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

(2)(a) [*The*] **A** consumer reporting agency shall send a written confirmation of a security freeze on a consumer's consumer report to the consumer at the last known address for the consumer shown in the consumer report that the consumer reporting agency maintains, within 10 business days after placing the security freeze and, with the confirmation, shall provide the consumer with a unique personal identification number or password or similar device the consumer must use to authorize the consumer reporting agency to release the consumer's consumer report for a specific period of time or to permanently remove the security freeze. The consumer reporting agency shall include with the written confirmation information that describes how to remove a security freeze and how to temporarily lift a security freeze on a consumer report, other than a consumer report for a protected consumer, in order to allow access to information from the consumer's consumer report for a period of time while the security freeze is in place.

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

(3)(a) If a consumer wishes to allow the consumer's consumer report to be accessed for a

specific period of time while a security freeze is in effect, the consumer shall contact the consumer reporting agency using a point of contact the consumer reporting agency designates, request that the security freeze be temporarily lifted and provide the following:

(A) Proper identification;

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

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

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

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

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

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

(a) Proper identification;

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

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

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

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

(A) Proper identification; **and**

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

[*(C) A fee, if applicable.*]

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

(A) Proper identification;

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

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

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

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

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

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

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

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

A consumer reporting agency may not charge a consumer a fee or collect from a consumer any money or item of value for:

(1) Placing, temporarily lifting or removing a security freeze on the consumer's consumer report.

(2) Creating or deleting a protective record.

(3) Placing or removing a security freeze on a protective record for a protected consumer.

(4) Replacing a lost personal identification number, password or similar device the consumer reporting agency previously provided to the consumer.

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

646A.622. (1) A person that owns, maintains or otherwise possesses**, or has control over or access to,** data that includes [*a consumer's*] personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information.

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

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

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

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

(d) Implements an information security program that includes:

(A) Administrative safeguards such as:

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

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

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

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

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

(vi) Adjusting the security program in light of business changes**, potential threats** or new circumstances; **and**

(vii) Reviewing user access privileges with reasonable regularity;

(B) Technical safeguards such as:

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

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

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

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

(iv) [*Testing and monitoring*] Regularly **testing, monitoring and taking action to address** the effectiveness of key controls, systems and procedures; and

(C) Physical safeguards such as:

(i) Assessing**, in light of current technology,** risks of information **collection,** storage**, usage, retention, access** and disposal **and implementing reasonable methods to remedy or mitigate identified risks**;

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

(iii) Protecting against unauthorized access to or use of personal information during or after collecting, **using, storing,** transporting, **retaining,** destroying or disposing of the personal information; and

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

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

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

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

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

Approved by the Governor March 16, 2018
Filed in the office of Secretary of State March 21, 2018
Effective date June 2, 2018