CHAPTER 357

AN ACT SB 601

Relating to enforcement of notification requirements for breaches of security involving personal information; creating new provisions; and amending ORS 646.607, 646A.602, 646A.604 and 646A.622.

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 [*October 1, 2007*] **the effective date of this 2015 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 [*October 1, 2007*] **the effective date of this 2015 Act**.

(5) "Debt" means any obligation or alleged obligation arising out of a consumer transaction[*, as defined in ORS 646.639*].

(6) "Encryption" means [*the use of*] an algorithmic process [*to transform*] **that renders** data [*into a form in which the data is rendered*] 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 form available from the Federal Trade Commission, or another substantially similar form.

(10) "Person" means [*any*] **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) "Personal information" **means**:

(a) [*Means*] 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** [*when the data elements are not rendered unusable through encryption, redaction or other methods, or when*] the data elements are encrypted and the encryption key has [*also*] been acquired:

(A) **A consumer's** Social Security number;

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

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

(D) **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[.]**;**

(E) 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) 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

(G) 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) [*Means*] Any of the data elements or any combination of the data elements described in paragraph (a) of this subsection [*when not combined with*] **without** the consumer's first name or first initial and last name [*and when the data elements are not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised.*] **if:**

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

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

(c) **"Personal information"** does not include information[*, other than a Social Security number,*] 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**,** [*or*] credit **card number** or debit card number is **visible or** accessible [*as part of the data*].

(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) [*Any*] **A** person that owns[*, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities and*] **or licenses 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 shall give notice of the breach of security [*following discovery of such breach of security, or receipt of notification under subsection (2) of this section, to any consumer whose personal information was included in the information that was breached. The disclosure notification shall be made in*] **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 [*time*] **manner** possible**,** [*and*] without unreasonable delay, consistent with the legitimate needs of law enforcement [*as provided*] **described** in subsection (3) of this section[*,*] and consistent with any measures **that are** necessary to determine sufficient contact information for the [*consumers*] **affected consumer**, determine the scope of the breach **of security** and restore the reasonable integrity, security and confidentiality of the [*data*] **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) [*Any*] **A** person that maintains or otherwise possesses personal information on behalf of**, or under license of,** another person shall notify the [*owner or licensor of the information of any breach of security immediately following discovery of such*] **other person after discovering a** breach of security [*if a consumer's personal information was included in the information that was breached*].

(3) [*The notification to the consumer required by this section may be delayed*] **A person that owns or licenses personal information may delay notifying a consumer of a breach of security only** if a law enforcement agency determines that [*the*] **a** notification will impede a criminal investigation and [*that*] **if the law enforcement** agency [*has made a written request that the notification be delayed*] **requests in writing that the person delay the notification**. [*The notification required by this section shall be made after that law enforcement agency determines that its disclosure will not compromise the investigation and notifies the person in writing.*]

(4) For purposes of this section, [*notification to the consumer may be provided by one of the following methods*] **a person that owns or licenses personal information may notify a consumer of a breach of security**:

[*(a) Written notice.*]

(a) In writing;

(b) [*Electronic notice*] **Electronically,** if the [*person's customary method of communication*] **person customarily communicates** with the consumer [*is by electronic means or*] **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 [*October 1, 2007.*] **the effective date of this 2015 Act;**

[*(c) Telephone notice, provided that contact is made directly with the affected consumer.*]

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

(d) **With** substitute notice, if the person demonstrates that the cost of [*providing notice*] **notification otherwise** would exceed $250,000[*,*] **or** that the

affected class of consumers [*to be notified*] exceeds 350,000, or if the person does not have sufficient contact information to [*provide notice*] **notify affected consumers**. **For the purposes of this paragraph, "**substitute notice**"** [*consists of the following*] **means**:

(A) [*Conspicuous*] Posting [*of*] the notice or a link to the notice **conspicuously** on the [*Internet home page of the person*] **person's website** if the person maintains [*one*] **a website**; and

(B) [*Notification to*] **Notifying** major statewide television and newspaper media.

(5) Notice under this section [*shall*] **must** include**,** at a minimum:

(a) A description of the [*incident*] **breach of security** in general terms;

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

(c) The type of personal information [*obtained as a result of*] **that was subject to** the breach of security;

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

(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 [*affecting*] **that affects** more than 1,000 consumers [*that requires disclosure under this section*], 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 [*notification given by*] **notice** the person **gave** to [*the*] **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**. [*In no case shall a person that is required to make a notification required by this section delay any notification in order to make the notification to the consumer reporting agencies. The person shall include the police report number, if available, in its notification to the consumer reporting agencies.*]

(7) Notwithstanding subsection (1) of this section, [*notification is not required*] **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 [*responsible for law enforcement*], the person **reasonably** determines that [*no reasonable likelihood of harm to*] the consumers whose personal information [*has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years*] **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) This section does not apply to:

(a) A person that complies with [*the*] notification requirements or [*breach of security*] 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** provide greater protection to personal information and **disclosure requirements** at least as thorough **as the protections and disclosure requirements provided under this section** [*disclosure requirements pursuant to the rules, regulations, procedures, guidance or guidelines established by the person's primary or functional federal regulator*].

(b) A person that complies with a state or federal law that provides greater protection to personal information and [*at least as thorough disclosure requirements for breach of security of personal information than that provided by*] **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 [*October 1, 2007.*] **the effective date of this 2015 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 the effective date of this 2015 Act, that is governed under 45 C.F.R. parts 160 and 164, as in effect on the effective date of this 2015 Act, if the covered entity sends the Attorney General a copy of the notice the covered entity sent to consumers under ORS 646A.604 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.

(9)(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.622 is amended to read:

646A.622. (1) [*Any*] **A** person that owns, maintains or otherwise possesses data that includes a

consumer's personal information that [*is used*] **the person uses** in the course of the person's business, vocation, occupation or volunteer activities [*must*] **shall** develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, [*including disposal of the data*] **including safeguards that protect the personal information when the person disposes of the personal information**.

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

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

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

(c) [*A person that is subject to and*] Complies with regulations [*implementing*] **that implement** the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164) as [*that Act existed on October 1, 2007*] **in effect on the effective date of this 2015 Act, if the person is subject to the Act**.

(d) [*A person that*] Implements an information security program that includes [*the following*]:

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

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

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

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

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

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

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

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

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

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

(iii) [*Detects, prevents and responds*] **Detecting, preventing and responding** to attacks or system failures; and

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

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

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

(ii) [*Detects, prevents and responds*] **Detecting, preventing and responding** to intrusions;

(iii) [*Protects*] **Protecting** against unauthorized access to or use of personal information during or after [*the collection, transportation and destruction or disposal of the*] **collecting, transporting, destroying or disposing of the personal** information; and

(iv) [*Disposes*] **Disposing** of personal information after [*it is no longer needed*] **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 [*to*] **for** the size and complexity of the small business, the nature and scope of [*its*] **the small business's** activities, and the sensitivity of the personal information [*collected*] **the small business collects** from or about consumers.

SECTION 4. ORS 646.607 is amended to read:

646.607. A person engages in an unlawful practice if in the course of the person's business, vocation or occupation the person:

(1) Employs any unconscionable tactic in connection with selling, renting or disposing of real estate, goods or services, or collecting or enforcing an obligation;

(2) Fails to deliver all or any portion of real estate, goods or services as promised, and at a customer's request, fails to refund money that the customer gave to the person to purchase the undelivered real estate, goods or services and that the person does not retain pursuant to any right, claim or defense the person may assert in good faith. This subsection does not create a warranty obligation and does not apply to a dispute over the quality of real estate, goods or services delivered to a customer;

(3) Violates ORS 401.965 (2);

(4) Violates a provision of ORS 646A.725 to 646A.750;

(5) Violates ORS 646A.530;

(6) Employs a collection practice that is unlawful under ORS 646.639;

(7) Is a beneficiary that violates ORS 86.726 (1)(a) or (2), 86.729 (4) or 86.732 (1) or (2); [*or*]

(8) Violates ORS 646A.093[.]**; or**

(9) Violates a provision of ORS 646A.600 to 646A.628.

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

Approved by the Governor June 10, 2015
Filed in the office of Secretary of State June 10, 2015
Effective date January 1, 2016