Senate Bill 684

Sponsored by COMMITTEE ON JUDICIARY

SUMMARY

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

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

A BILL FOR AN ACT

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

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

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

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

SECTION 2. ORS 646A.602, as amended by section 1, chapter 10, Oregon Laws 2018, 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 **or possesses**.

(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 [*June 2, 2018*] **the effective date of this 2019 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 [*June 2, 2018*] **the effective date of this 2019 Act**.

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

(b) "Covered entity" does not include a person described in paragraph (a) of this subsection to the extent that the person acts solely as a vendor.

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

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

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

[*(7)*] **(8)** "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)*] **(9)** "Identity theft" has the meaning set forth in ORS 165.800.

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

[*(10)*] **(11)** "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)*] **(12)(a)** "Personal information" means:

(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:

(i) A consumer's Social Security number;

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

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

(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;

(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;

(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; [*and*] **or**

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

[*(B)*] **(C)** Any of the data elements or any combination of the data elements described in subparagraph (A) **or (B)** of this paragraph without the consumer's **user name, or the consumer's** first name or first initial and last name**,** 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.

(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)*] **(13)** "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)*] **(14)** "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)*] **(15)** "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)*] **(16)** "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)*] **(17)** "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)*] **(18)** "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.

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

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

646A.604. (1) If a [*person owns, 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*] **covered entity is** subject to a breach of security or [*if the person received*] **receives** notice of a breach of security from [*another person that maintains or otherwise possesses personal information on the person's behalf*] **a vendor**, the [*person*] **covered entity** shall give notice of the breach of security to:

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

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

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

(2)(a) A vendor that discovers a breach of security or has reason to believe that a breach

of security has occurred shall notify a covered entity with which the vendor has a contract as soon as is practicable but not later than 10 days after discovering the breach of security or having a reason to believe that the breach of security occurred.

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

(c) A vendor shall notify the Attorney General in writing or electronically if the vendor was subject to a breach of security that involved the personal information of more than 250 customers or a number of customers that the vendor could not determine.

(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*] **A covered entity shall give notice of a breach of security** 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.

(b) [*In*] **Before** providing the notice **described in paragraph (a) of this subsection**, [*the person*] **a covered entity** 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.

[*(b)*] **(c)** A [*person that must give notice of a breach of security under this section*] **covered entity** may delay giving the notice **described in paragraph (a) of this subsection** 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*] **covered entity** delay the notification.

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

(a) In writing;

(b) Electronically, if the [*person*] **covered entity** 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 [*June 2, 2018*] **the effective date of this 2019 Act**;

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

(d) With substitute notice, if the [*person*] **covered entity** 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*] **covered entity** 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*] **covered entity's** website if the [*person*] **covered entity** 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 gave the notice*] **covered entity**;

(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*] **covered entity** discovers **or receives notice of** a breach of security that affects more than 1,000 consumers, the [*person*] **covered entity** 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*] **covered entity** gave to affected consumers and shall include in the notice any police report number assigned to the breach of security. A [*person*] **covered entity** may not delay notifying affected consumers of a breach of security in order to notify consumer reporting agencies.

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

(b) If a [*person*] **covered entity or an agent or affiliate of the covered entity** 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*] **covered entity, the agent or the affiliate** 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*] **covered entity, the agent or the affiliate** 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.

(8) Notwithstanding subsection (1) of this section, a [*person*] **covered entity** 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*] **covered entity** reasonably determines that the consumers whose personal information was subject to the breach of security are unlikely to suffer harm. The [*person*] **covered entity** must document the determination in writing and maintain the documentation for at least five years.

(9) This section does not apply to:

(a) **Personal information that is subject to, and** 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*] **personal information and the person would otherwise be subject to ORS 646A.600 to 646A.628**.

(b) **Personal information that is subject to, and** 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) **Personal information that is subject to, and** 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 [*June 2, 2018*] **the effective date of this 2019 Act,**

if the personal information and the person would otherwise be subject to ORS 646A.600 to 646A.628.

[*(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 June 2, 2018, that is governed under 45 C.F.R. parts 160 and 164, as in effect on June 2, 2018, 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.*]

(d) Personal information that is subject to, and a person that complies with, regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, 110 Stat. 1936) and the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5, Title XIII, 123 Stat. 226), as those Acts existed on the effective date of this 2019 Act, if the personal information and the person would otherwise be subject to ORS 646A.600 to 646A.628.

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

(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 4. ORS 646A.622, as amended by section 6, chapter 10, Oregon Laws 2018, 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 personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities*] **covered entity and a vendor** 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*] **covered entity or vendor** disposes of the personal information.

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

(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 [*June 2, 2018*] **the effective date of this 2019 Act**, if [*the person*] **personal information that is subject to ORS 646A.600 to 646A.628** is **also** 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 June 2, 2018,*] **and the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5, Title XIII, 123 Stat. 226), as those Acts were in effect on the effective date of this 2019 Act,** if [*the person*] **personal information that is subject to ORS 646A.600 to 646A.628** is **also** subject to [*the Act*] **those Acts**.

(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;

(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) 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) 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*] **covered entity or vendor** disposes of the personal information on or off the [*person's*] **covered entity's or vendor's** premises or property, after the [*person*] **covered entity or vendor** 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*] **covered entity or vendor** complies with subsection (2)(d)(C)(iv) of this section if the [*person*] **covered entity or vendor** 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 5. The amendments to ORS 646A.600, 646A.602, 646A.604 and 646A.622 by sections 1 to 4 of this 2019 Act apply to covered entities or vendors that own, license, maintain, store, manage, collect, process, acquire or otherwise possess personal information, or that have access to personal information as a consequence of a contract, on or after the effective date of this 2019 Act.