House Bill 2581

Sponsored by Representatives RAYFIELD, OLSON (Presession filed.)

SUMMARY

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

Requires person that possesses or has access to account information to report breach of security to financial institution that issued financial access device. Requires person to safeguard account information in accordance with standards that Department of Consumer and Business Services adopts by rule.

Subjects person to liability to financial institution for costs financial institution incurs as consequence of breach of security if person's failure to comply with standards for safeguarding account information amounts to gross negligence.

Becomes operative January 1, 2018.

Declares emergency, effective on passage.

A BILL FOR AN ACT

Relating to breaches of security with respect to account information associated with financial access devices; amending ORS 646A.602, 646A.604 and 646A.622; and declaring an emergency.

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) "Account information" means information that establishes a relationship between a consumer and the consumer's account with a financial institution including, but not limited to:

(a) A primary account number;

(b) The consumer's full name;

(c) The expiration date for the financial access device;

(d) A personal identification number or other security number; and

(e) A card verification value number, card security code number or similar security number.

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

[*(3)*] **(4)** "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 operative date specified in section 5 of this 2017 Act**, that a consumer reporting agency compiles and maintains.

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.

[*(4)*] **(5)** "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 operative date specified in section 5 of this 2017 Act**.

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

[*(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.

(9) "Financial access device" means a consumer's credit card or debit card or a similar or related device that a consumer uses in a transaction to make a payment that draws on an extension of credit to the consumer from a financial institution or that withdraws funds from an account the consumer maintains with a financial institution.

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

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

[*(9)*] **(12)** "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)*] **(13)** "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)*] **(14)** "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:

(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 identification number issued by the United States;

(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) Any of the data elements or any combination of the data elements described in paragraph (a) of this subsection without the consumer's first name or first initial and last name if:

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

(B) The data element or combination of data elements would enable a person to commit identity

theft against a consumer.

(c) Account information that is ordinarily stored on a financial access device.

[*(c)*] **(d)** "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)*] **(15)** "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)*] **(16)** "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)*] **(17)** "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)*] **(18)** "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)*] **(19)** "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)*] **(20)** "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 personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities**, or possesses or has access to personal information as a consequence of a transaction with a consumer,** and [*that*] **the personal information** was subject to a breach of security**, 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.

(c) The financial institution that issued a financial access device that stores account information that was subject to the breach of security.

(d) Any merchant services provider that processed a financial transaction on the person's behalf using account information that was subject to the breach of security.

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

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

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

(a) In writing;

(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 operative date specified in section 5 of this 2017 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**, or that possessed or had access to as a consequence of a transaction with a consumer,** 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 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 se-

curity in order to notify consumer reporting agencies.

(7) 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)(a) Subject to paragraph (b) of this subsection, if the personal information that was subject to the breach of security is account information, the person that owned or licensed the personal information, or that possessed or had access to the personal information as a consequence of a transaction with a consumer, is liable to the financial institution that issued the financial access device that stored the account information that was subject to the breach for costs the financial institution incurs with respect to:

(A) Canceling or reissuing the financial access device;

(B) Stopping payments or blocking transactions in order to protect a consumer's account;

(C) Closing or reopening a consumer's account with the financial institution;

(D) Refunding or crediting a consumer for a transaction that the consumer did not authorize and that occurred as a result of the breach of security; or

(E) Notifying the consumer about the breach of security.

(b) A person is liable to a financial institution under paragraph (a) of this subsection only if the person's failure to secure the account information in accordance with standards described in ORS 646A.622 (2)(d) amounted to gross negligence.

(c) A financial institution may bring an action in a court of this state to recover any costs described in paragraph (a) of this subsection that the financial institution incurred as a result of the person's failure to meet the standard specified in paragraph (b) of this subsection.

[*(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 provide 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 operative date specified in section 5 of this 2017 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 operative date specified in section 5 of this 2017 Act**, that is governed under 45 C.F.R. parts 160 and 164, as in effect on [*January 1, 2016*] **the operative date specified in section 5 of this 2017 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)*] **(10)(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) A person that owns, maintains or otherwise possesses **or has 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**, or possesses or has access to as a consequence of a transaction with a consumer,** 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 operative date specified in section 5 of this 2017 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 operative date specified in section 5 of this 2017 Act**, if the person is subject to the Act.

(d) Complies with security standards the Department of Consumer and Business Services adopts by rule for personal information that is account information. The rules that the department adopts under this paragraph must be consistent with, and not more stringent than, the security standards that the Payment Card Industry Security Standards Council, or a successor organization, adopts for safeguarding cardholder data. The department shall update the department's rules as needed to comply with this paragraph.

[*(d)*] **(e)** 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;

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

(iv) Training and managing employees in security program practices and procedures;

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

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

(B) Technical safeguards such as:

(i) Assessing risks in network and software design;

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

(iii) Detecting, preventing and responding to attacks or system failures; and

(iv) Testing and monitoring regularly the effectiveness of key controls, systems and procedures; and

(C) Physical safeguards such as:

(i) Assessing risks of information storage and disposal;

(ii) Detecting, preventing and responding to intrusions;

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

(iv) Disposing of personal information 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)*] **(2)(e)(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)*] **(2)(e)(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 4. The amendments to ORS 646A.602, 646A.604 and 646A.622 by sections 1 to 3 of this 2017 Act apply to transactions that occur on or after the operative date specified in section 5 of this 2017 Act.

SECTION 5. (1) The amendments to ORS 646A.602, 646A.604 and 646A.622 by sections 1 to 3 of this 2017 Act become operative January 1, 2018.

(2) The Department of Consumer and Business Services may adopt rules and take any other action before the operative date specified in subsection (1) of this section that is necessary to enable the department, on and after the operative date specified in subsection (1) of this section, to exercise all of the duties, functions and powers conferred on the department by the amendments to ORS 646A.602, 646A.604 and 646A.622 by sections 1 to 3 of this 2017 Act.

SECTION 6. This 2017 Act being necessary for the immediate preservation of the public peace, health and safety, an emergency is declared to exist, and this 2017 Act takes effect on its passage.
