House Bill 3411

Sponsored by Representative GOMBERG; Representatives BOONE, GALLEGOS, LIVELY, Senator ROBLAN

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.**

Expands circumstances under which breach of security requires notification under Oregon Consumer Identity Theft Protection Act to include disclosure of written data that contains personal information.

Requires person that owns, maintains or possesses written data that contains personal information to implement safeguards.

A BILL FOR AN ACT

Relating to protections for data that is subject to identity theft; creating new provisions; and amending ORS 646A.602 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)*] **(1)** "Breach of security" means **an** unauthorized acquisition of **written data or** computerized data that materially compromises the security, confidentiality or integrity of personal information [*maintained by the person*].

[*(b) "Breach of security" does not include good-faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person 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) "Computerized data" means information generated or stored by any electronic means on a computer or on any other electronic data processing or storage device or medium.

[*(2)*] **(3)** "Consumer" means an individual who is [*also*] a 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 October 1, 2007, that [*is compiled and maintained by*] a consumer reporting agency **compiles and maintains**.

[*(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 October 1, 2007.

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

[*(6)*] **(7)** "Encryption" means [*the use of*] an algorithmic process [*to transform*] **that transforms** data into a form in which the data is [*rendered*] unreadable or unusable without [*the use of*] **using** a confidential process or key.

[*(7)*] **(8)** "Extension of credit" means [*the*] **a** right **a person offers or grants to a consumer** to defer [*payment of*] **paying a** debt **the consumer incurs primarily for personal, family or household purposes,** or **a right the person grants to the consumer** to incur debt and defer **repaying**

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.

the debt [*its payment 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 [*documenting*] **that documents** alleged identity theft, using the form available from the Federal Trade Commission, or another substantially similar form.

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

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

[*(A)*] **(i) A** Social Security number;

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

[*(C)*] **(iii) A** passport number or other [*United States issued*] identification number **the United States issues**; or

[*(D)*] **(iv) A** financial account number, credit or debit card number, in combination with [*any*] **a** required security code, access code or password that would permit access to a consumer's financial account.

[*(b)*] **(B)** [*Means any of*] The data elements or [*any*] **a** combination of the data elements described in [*paragraph (a)*] **subparagraph (A)** of this [*subsection when not*] **paragraph even if the data elements are not** combined with the consumer's first name or first initial and last name and [*when*] **even if** the data elements are not rendered unusable through encryption, redaction or other methods, if the [*information obtained*] **data element or combination of data elements** would [*be sufficient to permit*] **enable** a person to commit identity theft against [*the*] **a** consumer [*whose information was compromised*].

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

[*(12)*] **(13)** "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, account number or credit or debit card number is accessible as part of the data.

[*(13)*] **(14)** "Security freeze" means a notice placed in a consumer report, at the **consumer's** request [*of a consumer*] and subject to certain exemptions, that prohibits [*the*] **a** consumer reporting agency from releasing the consumer report for [*the*] **an** extension of credit unless the consumer has temporarily lifted or removed the freeze.

(15) "Written data" means a paper, document, instrument, record, report, memorandum, communication, file or other tangible medium that embodies the data elements described in subsection (12)(a) of this section, whether the medium is original or a copy and regardless of the medium's physical form or characteristics.

SECTION 2. ORS 646A.622 is amended to read:

646A.622. (1) [*Any*] **A** person that owns, maintains or otherwise possesses **written data or computerized** data that includes a consumer's personal information **and** 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*] **safeguards that govern how the person may dispose of the data**.

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

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

(b) [*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**, if the person is subject to the federal 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**, if the person is subject to the federal Act**.

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

(A) Administrative safeguards**, including but not limited to** [*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*] **Assessing** the sufficiency of safeguards [*in place*] to control the identified risks;

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

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

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

(B) Technical safeguards**, including but not limited to** [*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** the effectiveness of key controls, systems and procedures **regularly**; and

(C) Physical safeguards**, including but not limited to** [*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*] **collecting, transporting and destroying or disposing of** the information; and

(iv) [*Disposes*] **Disposing** of personal information after [*it*] **the person no longer needs the personal information** [*is no longer needed*] for business purposes**,** or [*as required by*] **to meet** local, state or federal law **requirements,** by burning, pulverizing, shredding or modifying [*a physical record*] **written data** and by destroying or erasing [*electronic media*] **computerized data** so that the **personal** 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 **that is** engaged in the business of record destruction to dispose of personal information in a manner 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 appropriate to the size and complexity of the small business, the nature and scope of [*its*] **the** activities **of the small business**[,] and the sensitivity of the personal information collected from or about consumers.

SECTION 3. The amendments to ORS 646A.602 and 646A.622 by sections 1 and 2 of this 2013 Act apply to breaches of security that occur on or after the effective date of this 2013 Act.