House Bill 2858

Sponsored by Representative CLEM; Representatives BARKER, BEYER, BOONE, CANNON, DEMBROW, C EDWARDS, GALIZIO, GARRETT, GELSER, GREENLICK, HARKER, HOLVEY, KOMP, MATTHEWS, NATHANSON, READ, RILEY, ROBLAN, SCHAUFLER, J SMITH, STIEGLER, TOMEI, VANORMAN, WITT

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.**

Adds state and federal tax identification numbers to personal information subject to provisions of Oregon Consumer Identity Theft Protection Act. Requires mitigation of risks and losses for consumers and employees as part of measures to protect against breach of security that affects personal information. Applies requirements to all businesses.

A BILL FOR AN ACT

Relating to identity theft measures; 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)*] "Breach of security" means **an** unauthorized acquisition of 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) "Consumer" means an individual who is [*also*] a 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, that is compiled and maintained by a consumer reporting agency.

(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.

(5) "Debt" means [*any*] **an** 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 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 [*the*] **a** right **offered or granted primarily for personal, family or household purposes** to defer payment of debt or to incur debt and defer [*its*] payment**.** [*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 documenting alleged

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.

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":

(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 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) Social Security number **or state or federal tax identification number**;

(B) Driver license number or state identification card number issued by the Department of Transportation;

(C) Passport number or other United States issued identification number; or

(D) Financial account number, credit 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.

(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 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.

(c) Does not include information, other than a Social Security number **or state or federal tax identification number**, in a federal, state or local government record that is lawfully made available to the public.

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

SECTION 2. 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 in the course of the person's business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data.

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

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

[*(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.*]

[*(c) A person that is subject to and complies with regulations implementing 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.*]

[*(d)*] **(2)** A person **complies with the provisions of subsection (1) of this section if the person** [*that*] implements an information security program that includes the following **measures**:

[*(A)*] **(a)** Administrative safeguards**, including but not limited to:** [*such as the following, in which the person:*]

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

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

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

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

(E) Mitigating risks and losses for consumers and the person's employees;

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

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

[*(B)*] **(b)** Technical safeguards**, including but not limited to:** [*such as the following, in which the person:*]

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

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

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

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

[*(C)*] **(c)** Physical safeguards**, including but not limited to:** [*such as the following, in which the person:*]

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

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

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

[*(iv)*] **(D)** [*Disposes*] **Disposing** of personal information after [*it*] **the personal information** is no longer needed 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)(c)(D)** 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 consistent with subsection [*(2)(d)(C)(iv)*] **(2)(c)(D)** 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 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 2009 Act apply to information security programs that are in effect on or after the effective date of this 2009 Act.

1 _____