LC 3657
2015 Regular Session
2/18/15 (TSB/ps)

D R A F T

SUMMARY

Establishes private right of action for consumer that suffers ascertainable loss of money or property as result of person's failure to maintain reasonable safeguards to protect security, confidentiality and integrity of consumer's personal information.

Becomes operative January 1, 2016.

Declares emergency, effective on passage.

A BILL FOR AN ACT

Relating to enforcing safeguards required for consumer personal data; creating new provisions; amending ORS 646A.622; and declaring an emergency.

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

SECTION 1. 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*] **shall** develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including [*disposal*] **properly disposing** of the data.

(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

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.

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**, 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**, 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*] **that include**:

(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*] **that include**:

(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*] **that include**:

(i) [*Assesses*] **Assessing** risks [*of*] **associated with** 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*] **collecting, transporting, destroying or disposing** of the information; and

(iv) [*Disposes*] **Disposing** of personal information after [*it is no longer needed*] **the person no longer needs the 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 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 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 **the small business** [*collected*] **collects** from or about consumers.

(5)(a) A consumer that suffers an ascertainable loss of money or property, real or personal, as a result of a person's failure to comply

with the provisions of this section may bring an action in a court of this state to recover the consumer's actual damages or statutory damages of $200, whichever is greater. The court or the jury may award punitive damages and the court may provide any equitable relief the court considers necessary or proper.

(b) A consumer that brings an action under this subsection shall mail a copy of the complaint or other initial pleading to the Director of the Department of Consumer and Business Services at the time the action begins and, at the time the court renders any judgment in the action, shall mail a copy of the judgment to the director. Failing to mail a copy of the complaint or initial pleading to the director is not a jurisdictional defect, but a court may not enter judgment for the consumer until the consumer files proof of mailing with the court, which may include an affidavit or return receipt.

(c) The court may award reasonable attorney fees and costs at trial and on appeal to a prevailing consumer in an action under this subsection. The court may award attorney fees and costs at trial and on appeal to a prevailing defendant only if the court finds that an objectively reasonable basis for bringing the action or asserting the ground for appeal did not exist. A court may not award attorney fees and costs to a prevailing defendant if a consumer maintained an action under this subsection as a class action under ORCP 32.

(d) A consumer must bring an action under this subsection within one year after discovering the person's violation of this section. Notwithstanding this limitation, if the director begins a proceeding to enforce a violation of this section under ORS 646A.624, the proceeding tolls the limit set forth in this paragraph with respect to a consumer's action that is based in whole or in part on a matter the director sets forth in an investigation, order or other action in the director's proceeding for the period of time in which the proceeding is pending.

(e) A consumer may bring and maintain an action under this sub-

section as a class action. In a class action under this subsection:

(A) Class members may recover statutory damages only if the plaintiffs in the action establish that the class members have sustained an ascertainable loss of money or property as a result of the defendant's reckless or knowing failure to comply with the provisions of this section;

(B) The trier of fact may award punitive damages; and

(C) The court may award appropriate equitable relief.

SECTION 2. The amendments to ORS 646A.622 by section 1 of this 2015 Act apply to ascertainable losses of money or property that a consumer suffers on or after the operative date set forth in section 3 of this 2015 Act.

SECTION 3. (1) The amendments to ORS 646A.622 by section 1 of this 2015 Act become operative January 1, 2016.

(2) The Director of the Department of Consumer and Business Services, before the operative date specified in subsection (1) of this section, may adopt rules or take any other action that is necessary to enable the director, 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 director by the amendments to ORS 646A.622 by section 1 of this 2015 Act.

SECTION 4. This 2015 Act being necessary for the immediate preservation of the public peace, health and safety, an emergency is declared to exist, and this 2015 Act takes effect on its passage.
