House Bill 2442

Sponsored by Representative HANNA (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 business that owns, possesses or uses personal information to notify individual when breach of security that may result in misuse of personal information occurs.

Requires Department of Consumer and Business Services to establish registry of businesses that own, possess or use personal information.

Requires business that owns, possesses or uses personal information to provide individual, upon request, with copy of personal information about individual maintained by business.

Requires certain businesses to establish security system that protects personal information.

Allows private cause of action for damages.

Makes violation of certain provisions unlawful trade practice. Imposes maximum $90 fine for violation of certain provisions.

A BILL FOR AN ACT

Relating to security of personal information; creating new provisions; and amending ORS 646.608 and 646.990.

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

SECTION 1. As used in sections 1 to 5 of this 2007 Act:

(1) "Breach of security of noncomputerized data" means theft or unauthorized photocopying, transmission by facsimile or photographing of personal information maintained in paper or other nonelectronic format.

(2)(a) "Breach of security of system data" means unauthorized acquisition of computerized data that harms or poses an actual threat to the security, confidentiality or integrity of personal information maintained by a business.

(b) "Breach of security of system data" does not include good-faith acquisition of personal information by an employee or agent of a business for a legitimate purpose of that business 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.

(3) "Business" means any individual, private or public corporation, partnership, cooperative, association, estate, limited liability company, organization, public body as defined in ORS 174.109 or other entity that owns, possesses or uses personal information.

(4) "Contact person" means an agent or an employee of a business who is authorized by the business to provide information.

(5)(a) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(A) Date of birth;

(B) Social Security number;

(C) Driver license or state identification card number;

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.

(D) Passport number; or

(E) Account number, credit or debit card number, security code, access code or password that would permit access to the individual's financial account.

(b) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

SECTION 2. (1) Upon discovery of a breach of security of noncomputerized data or a breach of security of system data, a business that owns, possesses or uses the data shall assess the nature and scope of the incident and identify the personal information systems and types of personal information that have been accessed or misused. If the business determines that misuse of personal information about an individual with a mailing address in this state has occurred or that it is reasonably possible that misuse may occur, the business shall provide notification of the breach to:

(a) Appropriate law enforcement agencies;

(b) The primary state regulator of the business, if any; and

(c) The individual with a mailing address in this state. The notification to the individual may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation or prosecution and provides the business that sustained the breach with a written request for the delay. The business must promptly notify the individual as soon as notification no longer interferes with the investigation or prosecution.

(2) The business shall notify the individual described in subsection (1) of this section as expeditiously as possible, consistent with the legitimate needs of law enforcement agencies as described in subsection (1) of this section, or any measures necessary for the business to determine the scope of the breach and restore reasonable integrity of the data system.

(3) Subsection (1) of this section does not apply to a financial institution, as defined in ORS 706.008, that complies with regulations or guidance issued by its regulator concerning notification upon discovery of a breach of security of noncomputerized data or a breach of security of system data.

(4) The business shall deliver the notification to the individual described in subsection (1) of this section in any manner designed to ensure that an individual can reasonably be expected to receive it. The notification must:

(a) Describe the incident in general terms and the type of personal information about an individual that was the subject of the breach;

(b) Advise an individual of the need to remain vigilant to possible identity theft;

(c) Advise an individual to promptly report incidents of suspected identity theft to law enforcement agencies; and

(d) Provide information about the Federal Trade Commission's online guidance regarding steps an individual can take to protect against identity theft.

SECTION 3. (1) The Department of Consumer and Business Services shall establish a registry of all businesses that own, possess or use personal information.

(2) For the purpose of establishing and maintaining the registry described in subsection (1) of this section, each business described in subsection (1) of this section shall notify the department of the name and address of the business and the name of a contact person within the business.

(3) The department shall provide an individual with the name of each business in the

registry upon written request of the individual.

SECTION 4. (1) An individual may request in writing that a contact person provide a copy of all personal information about the individual maintained by a business regardless of whether there has been a breach of security of noncomputerized data or a breach of security of system data.

(2) A business shall adopt procedures to verify the identity of the individual and to ensure that the individual requesting the personal information is authorized to receive the personal information.

(3) A business shall provide the personal information sought by the individual within a reasonable time after receipt of the written request.

SECTION 5. (1) A business that owns, possesses or uses computerized data systems that contain personal information shall establish a security system to safeguard the personal information.

(2) The security system shall include:

(a) Installing and maintaining a firewall configuration that protects data by preventing unauthorized access to stored data from outside and inside the business's network;

(b) Changing vendor-supplied default passwords and security parameters before installing a new data system;

(c) Minimizing the amount of data stored on a network and storing retained data in encrypted formats;

(d) Encrypting transmission of data and sensitive information across public networks;

(e) Using and regularly updating antivirus software;

(f) Restricting access to data to individuals who need access to fulfill job functions;

(g) Assigning a unique identification to each individual with access to data;

(h) Restricting physical access to data systems to prevent unauthorized removal of systems or copies of data;

(i) Establishing and maintaining a security policy that defines information security responsibilities;

(j) Testing systems and processes on a regular basis to ensure the identification and blocking of unauthorized access attempts; and

(k) Tracking and monitoring of all access to network resources, in a manner that automatically creates audit trails for individual user access and other system activities that could indicate tampering attempts.

SECTION 6. (1) An individual with a mailing address in this state who is injured by a violation of any provision of section 2 of this 2007 Act may bring a civil action to recover actual damages arising from the violation, or $2,500, whichever is greater.

(2) Except as provided in subsection (3) of this section, an action under this section must be brought within two years of the date the individual knew, or should have known, of the violation.

(3) When a defendant has materially and willfully misrepresented or failed to disclose any information required under section 2 of this 2007 Act to be disclosed to an individual and the information is material to the establishment of the defendant's liability to the individual, the action may be brought at any time within two years after the discovery by the individual of the misrepresentation of or failure to disclose the required information.

SECTION 7. ORS 646.608 is amended to read:

646.608. (1) A person engages in an unlawful practice when in the course of the person's business, vocation or occupation the person does any of the following:

(a) Passes off real estate, goods or services as those of another.

(b) Causes likelihood of confusion or of misunderstanding as to the source, sponsorship, approval, or certification of real estate, goods or services.

(c) Causes likelihood of confusion or of misunderstanding as to affiliation, connection, or association with, or certification by, another.

(d) Uses deceptive representations or designations of geographic origin in connection with real estate, goods or services.

(e) Represents that real estate, goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, quantities or qualities that they do not have or that a person has a sponsorship, approval, status, qualification, affiliation, or connection that the person does not have.

(f) Represents that real estate or goods are original or new if they are deteriorated, altered, reconditioned, reclaimed, used or secondhand.

(g) Represents that real estate, goods or services are of a particular standard, quality, or grade, or that real estate or goods are of a particular style or model, if they are of another.

(h) Disparages the real estate, goods, services, property or business of a customer or another by false or misleading representations of fact.

(i) Advertises real estate, goods or services with intent not to provide them as advertised, or with intent not to supply reasonably expectable public demand, unless the advertisement discloses a limitation of quantity.

(j) Makes false or misleading representations of fact concerning the reasons for, existence of, or amounts of price reductions.

(k) Makes false or misleading representations concerning credit availability or the nature of the transaction or obligation incurred.

(L) Makes false or misleading representations relating to commissions or other compensation to be paid in exchange for permitting real estate, goods or services to be used for model or demonstration purposes or in exchange for submitting names of potential customers.

(m) Performs service on or dismantles any goods or real estate when not authorized by the owner or apparent owner thereof.

(n) Solicits potential customers by telephone or door to door as a seller unless the person provides the information required under ORS 646.611.

(o) In a sale, rental or other disposition of real estate, goods or services, gives or offers to give a rebate or discount or otherwise pays or offers to pay value to the customer in consideration of the customer giving to the person the names of prospective purchasers, lessees, or borrowers, or otherwise aiding the person in making a sale, lease, or loan to another person, if earning the rebate, discount or other value is contingent upon occurrence of an event subsequent to the time the customer enters into the transaction.

(p) Makes any false or misleading statement about a prize, contest or promotion used to publicize a product, business or service.

(q) Promises to deliver real estate, goods or services within a certain period of time with intent not to deliver them as promised.

(r) Organizes or induces or attempts to induce membership in a pyramid club.

(s) Makes false or misleading representations of fact concerning the offering price of, or the person's cost for real estate, goods or services.

(t) Concurrent with tender or delivery of any real estate, goods or services fails to disclose any known material defect or material nonconformity.

(u) Engages in any other unfair or deceptive conduct in trade or commerce.

(v) Violates any of the provisions relating to auction sales, auctioneers or auction marts under ORS 698.640, whether in a commercial or noncommercial situation.

(w) Manufactures mercury fever thermometers.

(x) Sells or supplies mercury fever thermometers unless the thermometer is required by federal law, or is:

(A) Prescribed by a person licensed under ORS chapter 677; and

(B) Supplied with instructions on the careful handling of the thermometer to avoid breakage and on the proper cleanup of mercury should breakage occur.

(y) Sells a thermostat that contains mercury unless the thermostat is labeled in a manner to inform the purchaser that mercury is present in the thermostat and that the thermostat may not be disposed of until the mercury is removed, reused, recycled or otherwise managed to ensure that the mercury does not become part of the solid waste stream or wastewater. For purposes of this paragraph, "thermostat" means a device commonly used to sense and, through electrical communication with heating, cooling or ventilation equipment, control room temperature.

(z) Sells or offers for sale a motor vehicle manufactured after January 1, 2006, that contains mercury light switches.

(aa) Violates the provisions of ORS 803.375, 803.385 or 815.410 to 815.430.

(bb) Violates ORS 646.850 (1).

(cc) Violates any requirement of ORS 646.661 to 646.686.

(dd) Violates the provisions of ORS 128.801 to 128.898.

(ee) Violates ORS 646.883 or 646.885.

(ff) Violates any provision of ORS 646.195.

(gg) Violates ORS 646.569.

(hh) Violates the provisions of ORS 646.859.

(ii) Violates ORS 759.290.

(jj) Violates ORS 646.872.

(kk) Violates ORS 646.553 or 646.557 or any rule adopted pursuant thereto.

(LL) Violates ORS 646.563.

(mm) Violates ORS 759.690 or any rule adopted pursuant thereto.

(nn) Violates the provisions of ORS 759.705, 759.710 and 759.720 or any rule adopted pursuant thereto.

(oo) Violates ORS 646.892 or 646.894.

(pp) Violates any provision of ORS 646.249 to 646.259.

(qq) Violates ORS 646.384.

(rr) Violates ORS 646.871.

(ss) Violates ORS 822.046.

(tt) Violates ORS 128.001.

(uu) Violates ORS 646.649 (2) to (4).

(vv) Violates ORS 646.877 (2) to (4).

(ww) Violates ORS 87.686.

(xx) Violates ORS 646.651.

(yy) Violates ORS 646.879.

(zz) Violates ORS 646.402 or any rule adopted under ORS 646.402 or 646.404.

(aaa) Violates ORS 180.440 (1).

(bbb) Commits the offense of acting as a vehicle dealer without a certificate under ORS 822.005.

(ccc) Violates ORS 87.007 (2) or (3).

(ddd) Violates ORS 92.405 (1), (2) or (3).

(eee) Engages in an unlawful practice under ORS 646.648.

(fff) Violates section 2 or 3 of this 2007 Act.

(2) A representation under subsection (1) of this section or ORS 646.607 may be any manifestation of any assertion by words or conduct, including, but not limited to, a failure to disclose a fact.

(3) In order to prevail in an action or suit under ORS 646.605 to 646.652, a prosecuting attorney need not prove competition between the parties or actual confusion or misunderstanding.

(4) An action or suit may not be brought under subsection (1)(u) of this section unless the Attorney General has first established a rule in accordance with the provisions of ORS chapter 183 declaring the conduct to be unfair or deceptive in trade or commerce.

(5) Notwithstanding any other provision of ORS 646.605 to 646.652, if an action or suit is brought under subsection (1)(aaa) of this section by a person other than a prosecuting attorney, relief is limited to an injunction and the prevailing party may be awarded reasonable attorney fees.

SECTION 8. ORS 646.990 is amended to read:

646.990. (1) Each violation of any of the provisions of ORS 646.010 to 646.180 by any person, firm or corporation, whether as principal, agent, officer or director, is punishable, upon conviction, by a fine of not less than $100 nor more than $500, or by imprisonment in the county jail not exceeding six months, or by both.

(2) Violation of ORS 646.725 or 646.730 is a Class A misdemeanor.

(3) Any person who willfully and intentionally violates any provision of ORS 646.895 to 646.899 shall be punished by a fine of not more than $1,000 or by imprisonment for not more than six months or both. Violation of any order or injunction issued pursuant to ORS 646.899 (1) shall constitute prima facie proof of a violation of this subsection.

(4) Violation of ORS 646.910 is a Class D violation.

(5) Violation of ORS 646.915 is a Class D violation.

(6) Violation of ORS 646.920 is a Class D violation.

(7) [*A person violating ORS 646.930 commits*] **Violation of ORS 646.930 is** a Class C misdemeanor.

(8) Violation of section 4 or 5 of this 2007 Act is a Class D violation.

SECTION 9. (1) Section 2 of this 2007 Act applies to breaches of security that occur on or after the effective date of this 2007 Act.

(2) Section 6 of this 2007 Act and the amendments to ORS 646.608 and 646.990 by sections 7 and 8 of this 2007 Act apply to violations that occur on or after the effective date of this 2007 Act.

SECTION 10. Section 3 of this 2007 Act becomes operative on July 1, 2008.