

# Senate Bill 1057

Sponsored by COMMITTEE ON RULES

## 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 owns or uses personal information to notify individual and consumer reporting agencies when there is breach of security that may result in misuse of personal information.

Requires consumer reporting agency receiving notice of potential misuse of personal information to place security alert in relevant credit reports.

Requires consumer reporting agency, at request of consumer, to place security freeze on consumer reports about consumer. Creates exceptions to requirements.

Prohibits disclosure of Social Security number of individual. Provides exceptions. Punishes violation by maximum of one year's imprisonment, \$6,250 fine, or both.

Requires person maintaining or possessing records containing personal information to take measures to protect against unauthorized access to or use of information prior to disposal or destruction of information.

Allows private cause of action for damages.

Makes violation of provisions of Act unlawful trade practice.

## A BILL FOR AN ACT

1 Relating to security of personal information; creating new provisions; and amending ORS 646.607.

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

3 **SECTION 1. As used in sections 1 to 8 of this 2005 Act:**

4 (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.

5 (2)(a) **"Breach of security of system data"** means acquisition of computerized data by an unauthorized person that harms or poses an actual threat to the security, confidentiality or 6 integrity of personal information maintained by a person.

7 (b) **"Breach of security of system data"** does not include good-faith acquisition of personal information by a 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 8 harms or poses an actual threat to the security, confidentiality or integrity of the personal information.

9 (3) **"Person"** means any individual, private or public corporation, partnership, cooperative, 10 association, estate, limited liability company, organization, public body as defined in ORS 174.109 or other entity.

11 (4)(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 12 name or the data elements are not encrypted or redacted:

13 (A) Date of birth;

14 (B) Social Security number;

15 (C) Driver license or state identification card number;

16 (D) Passport number; or

17 **NOTE:** Matter in **boldfaced** type in an amended section is new; matter *[italic and bracketed]* is existing law to be omitted. 18 New sections are in **boldfaced** type.

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

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

5       (5) "Security alert" means a notice placed in a consumer's credit report that notifies a  
6 recipient of the credit report that the consumer may be a victim of fraud.

7       (6) "Security freeze" means a notice placed in a consumer's credit report at the request  
8 of the consumer that prohibits the consumer reporting agency, except as provided in section  
9 4 of this 2005 Act, from releasing the consumer's credit report or any information from the  
10 credit report without the express authorization of the consumer.

11       SECTION 2. (1) Upon discovery of a breach of security of noncomputerized data or a  
12 breach of security of system data, a person that owns, possesses or uses the data shall as-  
13 sess the nature and scope of the incident and identify what personal information systems and  
14 types of personal information have been accessed or misused. If the person that maintains  
15 personal information determines that misuse of personal information about a consumer with  
16 a mailing address in this state has occurred or that it is reasonably possible that misuse  
17 may occur, the person shall provide notification of the breach as soon as possible after the  
18 discovery to:

19       (a) Appropriate law enforcement agencies;

20       (b) The person's primary state regulator, if any;

21       (c) Each consumer reporting agency described in section 603(p) of the federal Fair Credit  
22 Reporting Act as in effect on January 1, 2005; and

23       (d) The consumer with a mailing address in this state. The notification to the consumer  
24 may be delayed if an appropriate law enforcement agency determines that notification will  
25 interfere with a criminal investigation or prosecution and provides the person that sustained  
26 the breach of security with a written request for the delay. The person must promptly notify  
27 the consumer as soon as notification no longer interferes with the investigation or prose-  
28 cution.

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

33       (3) Consumer notification shall be delivered in any manner designed to ensure that a  
34 consumer can reasonably be expected to receive it. The notification shall:

35       (a) Describe the incident in general terms and the type of personal information about a  
36 consumer that was the subject of unauthorized access or use;

37       (b) Advise a consumer of the need to remain vigilant to possible identity theft;

38       (c) Advise a consumer to promptly report incidents of suspected identity theft to law  
39 enforcement authorities;

40       (d) Advise a consumer of the ability of the consumer to place a security freeze on the  
41 consumer's credit report under section 4 of this 2005 Act; and

42       (e) Provide information about the Federal Trade Commission's online guidance regarding  
43 steps a consumer can take to protect against identity theft.

44       SECTION 3. (1) Not later than five business days after receiving notification under sec-  
45 tion 2 of this 2005 Act, each consumer reporting agency shall place a security alert in the

1 credit report of each consumer with a mailing address in this state:

2 (a) Who is identified in the notification; and

3 (b) For whom the consumer reporting agency maintains a record.

4 (2) For a period of not less than 180 days beginning on the date the notification was re-  
5 ceived, each consumer reporting agency shall notify each person requesting consumer credit  
6 information with respect to a consumer of the existence of a security alert in that consum-  
7 er's credit report, regardless of whether a full credit report, credit score or summary report  
8 is requested.

9 (3) The placement of a security alert may not be used against a consumer in rating or  
10 determining creditworthiness.

11 **SECTION 4.** (1) Any consumer with a mailing address in this state who believes the  
12 consumer's personal identification may have been stolen or who receives notification under  
13 section 2 of this 2005 Act may place a security freeze in the consumer's credit report within  
14 90 days of the discovery of the possible theft or receipt of notification. The consumer may  
15 place the security freeze by making a request in writing by certified mail to a consumer re-  
16 porting agency.

17 (2) A consumer reporting agency shall place a security freeze in the consumer's credit  
18 report within five business days after receiving a consumer's request under subsection (1)  
19 of this section. The consumer reporting agency shall send a written confirmation of the se-  
20 curity freeze and a unique personal identification number or password to the consumer  
21 within 14 business days after receiving the consumer's request. The written confirmation  
22 shall describe the procedures for temporarily lifting or removing the security freeze.

23 (3) If a security freeze is in place, the consumer reporting agency may not release in-  
24 formation from a consumer's credit report to a third party without the consumer's express  
25 authorization, except as provided in subsection (4) of this section.

26 (4) While a security freeze is in place in a consumer's credit report, a credit reporting  
27 agency may provide information from that report without the consumer's consent when the  
28 person requesting the consumer report is:

29 (a) A person or a subsidiary, agent or assignee of the person with which the consumer  
30 has or, prior to assignment, had an account, contract or debtor-creditor relationship;

31 (b) Any state or local government agency, law enforcement agency, trial court or private  
32 collection agency acting pursuant to a court order or warrant; or

33 (c) A person making firm offers of credit or insurance from prescreened lists as provided  
34 for by the federal Fair Credit Reporting Act as in effect on January 1, 2005.

35 (5)(a) To permit access to a credit report by a third party or by all persons for a specified  
36 period of time, the consumer who requested the security freeze must contact the consumer  
37 reporting agency and request a temporary lift. The consumer shall include in the request the  
38 consumer's unique personal identification number or password provided by the credit re-  
39 porting agency and information regarding the third party or the period of time to which the  
40 temporary lift applies.

41 (b) The request for a temporary lift may be made by telephone, mail, facsimile, or elec-  
42 tronic mail pursuant to reasonable procedures established by the credit reporting agency.

43 (c) The consumer reporting agency must act upon the request for a temporary lift within  
44 three business days of receiving the request from the consumer.

45 (6) A security freeze shall remain in a consumer's credit report until the earlier of one

1 year from the date of the request or the date the consumer makes a written request for  
2 removal. If a consumer requests removal of a security freeze, the consumer must include  
3 with the request the consumer's unique personal identification number or password provided  
4 by the credit reporting agency. The credit reporting agency shall remove the security freeze  
5 from the consumer's credit report within three business days of receiving the written re-  
6 quest.

7 (7) A consumer may renew a security freeze request by submitting a written request that  
8 includes the consumer's unique personal identification number or password provided by the  
9 credit reporting agency.

10 (8) Except as provided in subsection (9) of this section, a consumer reporting agency may  
11 charge a consumer no more than \$10 for each placement, temporary lift, renewal or removal  
12 of a security freeze as described in this section.

13 (9) A consumer reporting agency may not charge a fee for placing a security freeze if the  
14 request for the freeze is made as a result of a breach of security of noncomputerized data  
15 or a breach of security of system data.

16 **SECTION 5.** (1) Except as provided in subsection (2) of this section, a person may not  
17 intentionally communicate or directly or indirectly display, transfer, sell, lease, loan, trade,  
18 rent or otherwise disclose any individual's Social Security number to a third party or to the  
19 general public without the affirmatively expressed consent of the individual.

20 (2) Nothing in this section prohibits or limits the display or transfer of a Social Security  
21 number:

22 (a) Required, authorized or excepted under any federal or state law;

23 (b) For a public health purpose, including the protection of the health or safety of an  
24 individual in an emergency situation;

25 (c) For a law enforcement purpose, including the investigation of fraud and the enforce-  
26 ment of a child support obligation;

27 (d) If the display is for a use occurring as a result of a legal interaction between busi-  
28 nesses, governments or a business and government, regardless of which entity initiates the  
29 interaction, including, but not limited to:

30 (A) The prevention of fraud, including fraud in protecting an employee's right to em-  
31 ployment benefits;

32 (B) The facilitation of credit checks or the facilitation of background checks of employ-  
33 ees, prospective employees or volunteers; or

34 (C) When the transmission of the Social Security number is incidental to, and in the  
35 course of, the sale, lease, franchising or merger of all or a portion of a business;

36 (e) If the transfer is part of a data-matching program involving a federal, state or local  
37 government agency;

38 (f) If the Social Security number is required to be submitted as part of an individual's  
39 application for any type of federal, state or local government benefit or program; or

40 (g) For internal verification or administrative purposes by a person's employee or agent  
41 for a legitimate purpose of that person, provided that the Social Security number is not used  
42 in violation of applicable law.

43 **SECTION 6.** A person who, in the course of business, maintains or otherwise possesses  
44 personal information, including disposal companies explicitly hired to dispose of records, may  
45 not dispose of or otherwise destroy a record containing personal information unless the

1 person takes reasonable measures to protect against unauthorized access to or use of the  
2 information in connection with or after disposal of the information. Reasonable measures  
3 include, but are not limited to:

- 4 (1) Burning, pulverizing, shredding or modifying the record containing personal informa-  
5 tion so that the information cannot be read or reconstructed;
- 6 (2) Destroying or erasing electronic media and other nonpaper media containing personal  
7 information so that the information cannot be read or reconstructed;
- 8 (3) Contracting with a person engaged in the business of record destruction to dispose  
9 of personal information in a manner consistent with this section; or
- 10 (4) Protecting against unauthorized access to or use of personal information during or  
11 after the collection, transportation and destruction of the information.

12 **SECTION 7.** (1) Any consumer with a mailing address in this state injured by a violation  
13 of any provision of section 2, 3, 4, 5 or 6 of this 2005 Act may bring a civil action to recover  
14 actual damages arising from the violation, or \$2,500, whichever is greater.

15 (2) Except as provided in this subsection, an action under this section must be brought  
16 within two years of the date the consumer knew, or should have known, of the violation.  
17 When a defendant has materially and willfully misrepresented or failed to disclose any in-  
18 formation required under section 2, 3, 4, 5 or 6 of this 2005 Act to be disclosed to a consumer  
19 and the information is material to the establishment of the defendant's liability to the con-  
20 sumer, the action may be brought at any time within two years after the discovery by the  
21 consumer of the misrepresentation or failure to disclose the required information.

22 **SECTION 8.** Violation of section 5 of this 2005 Act is a Class A misdemeanor.

23 **SECTION 9.** ORS 646.607 is amended to read:

24 646.607. A person engages in an unlawful practice when in the course of the person's business,  
25 vocation or occupation the person:

- 26 (1) Employs any unconscionable tactic in connection with sale, rental or other disposition of real  
estate, goods or services, or collection or enforcement of an obligation;
- 27 (2) Violates section 3, chapter 759, Oregon Laws 2003; [or]
- 28 (3) Fails to deliver all or any portion of real estate, goods or services as promised, and upon  
request of the customer, fails to refund any money that has been received from the customer that  
was for the purchase of the undelivered real estate, goods or services and that is not retained by  
the seller pursuant to any right, claim or defense asserted in good faith. This subsection does not  
create a warranty obligation and does not apply to a dispute over the quality of real estate, goods  
or services delivered to a customer[.]; or
- 29 (4) Violates section 2, 3, 4, 5 or 6 of this 2005 Act.

30 **SECTION 10.** ORS 646.607, as amended by section 10, chapter 759, Oregon Laws 2003, is  
31 amended to read:

32 646.607. A person engages in an unlawful practice when in the course of the person's business,  
33 vocation or occupation the person:

- 34 (1) Employs any unconscionable tactic in connection with sale, rental or other disposition of real  
estate, goods or services, or collection or enforcement of an obligation; [or]
- 35 (2) Fails to deliver all or any portion of real estate, goods or services as promised, and upon  
request of the customer, fails to refund any money that has been received from the customer that  
was for the purchase of the undelivered real estate, goods or services and that is not retained by  
the seller pursuant to any right, claim or defense asserted in good faith. This subsection does not

1 create a warranty obligation and does not apply to a dispute over the quality of real estate, goods  
2 or services delivered to a customer[.]; or  
3 **(3) Violates section 2, 3, 4, 5 or 6 of this 2005 Act.**  
4 **SECTION 11. (1) Sections 2 and 3 of this 2005 apply to breaches of security that occur**  
5 **on or after the effective date of this 2005 Act.**  
6 **(2) Sections 5 and 8 of this 2005 Act apply to communications, displays or transfers of**  
7 **Social Security numbers that occur on or after the effective date of this 2005 Act.**  
8 **(3) Section 6 of this 2005 Act applies to personal information to be disposed of on or after**  
9 **the effective date of this 2005 Act.**  
10 **(4) Section 7 and the amendments to ORS 646.607 by sections 9 and 10 of this 2005 Act**  
11 **apply to violations that occur on or after the effective date of this 2005 Act.**  
12

---