

646A.604 Notice of breach of security; delay; methods of notification; contents of notice; application of notice requirement. (1) A person that owns or licenses personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities and that was subject to a breach of security shall give notice of the breach of security to:

(a) The consumer to whom the personal information pertains after the person discovers the breach of security or after the person receives notice of a breach of security under subsection (2) of this section. The person shall notify the consumer in the most expeditious manner possible, without unreasonable delay, consistent with the legitimate needs of law enforcement described in subsection (3) of this section and consistent with any measures that are necessary to determine sufficient contact information for the affected consumer, determine the scope of the breach of security and restore the reasonable integrity, security and confidentiality of the personal information.

(b) The Attorney General, either in writing or electronically, if the number of consumers to whom the person must send the notice described in paragraph (a) of this subsection exceeds 250. The person shall disclose the breach of security to the Attorney General in the manner described in paragraph (a) of this subsection.

(2) A person that maintains or otherwise possesses personal information on behalf of, or under license of, another person shall notify the other person after discovering a breach of security.

(3) A person that owns or licenses personal information may delay notifying a consumer of a breach of security only if a law enforcement agency determines that a notification will impede a criminal investigation and if the law enforcement agency requests in writing that the person delay the notification.

(4) For purposes of this section, a person that owns or licenses personal information may notify a consumer of a breach of security:

(a) In writing;

(b) Electronically, if the person customarily communicates with the consumer electronically or if the notice is consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001) as that Act existed on January 1, 2016;

(c) By telephone, if the person contacts the affected consumer directly; or

(d) With substitute notice, if the person demonstrates that the cost of notification otherwise would exceed \$250,000 or that the affected class of consumers exceeds 350,000, or if the person does not have sufficient contact information to notify affected consumers. For the purposes of this paragraph, "substitute notice" means:

(A) Posting the notice or a link to the notice conspicuously on the person's website if the person maintains a website; and

(B) Notifying major statewide television and newspaper media.

(5) Notice under this section must include, at a minimum:

(a) A description of the breach of security in general terms;

(b) The approximate date of the breach of security;

(c) The type of personal information that was subject to the breach of security;

(d) Contact information for the person that owned or licensed the personal information that was subject to the breach of security;

(e) Contact information for national consumer reporting agencies; and

(f) Advice to the consumer to report suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission.

(6) If a person discovers a breach of security that affects more than 1,000 consumers, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain reports on consumers on a nationwide basis of the timing, distribution and content of the notice the person gave to affected consumers and shall include in the notice any police report number assigned

to the breach of security. A person may not delay notifying affected consumers of a breach of security in order to notify consumer reporting agencies.

(7) Notwithstanding subsection (1) of this section, a person does not need to notify consumers of a breach of security if, after an appropriate investigation or after consultation with relevant federal, state or local law enforcement agencies, the person reasonably determines that the consumers whose personal information was subject to the breach of security are unlikely to suffer harm. The person must document the determination in writing and maintain the documentation for at least five years.

(8) This section does not apply to:

(a) A person that complies with notification requirements or procedures for a breach of security that the person's primary or functional federal regulator adopts, promulgates or issues in rules, regulations, procedures, guidelines or guidance, if the rules, regulations, procedures, guidelines or guidance provide greater protection to personal information and disclosure requirements at least as thorough as the protections and disclosure requirements provided under this section.

(b) A person that complies with a state or federal law that provides greater protection to personal information and disclosure requirements at least as thorough as the protections and disclosure requirements provided under this section.

(c) 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 January 1, 2016.

(d)(A) Except as provided in subparagraph (B) of this paragraph, a covered entity, as defined in 45 C.F.R. 160.103, as in effect on January 1, 2016, that is governed under 45 C.F.R. parts 160 and 164, as in effect on January 1, 2016, if the covered entity sends the Attorney General a copy of the notice the covered entity sent to consumers under ORS 646A.604 or a copy of the notice that the covered entity sent to the primary functional regulator designated for the covered entity under the Health Insurance Portability and Availability Act of 1996, (P.L. 104-191, 110 Stat. 1936, 42 U.S.C. 300(gg), 29 U.S.C. 118 et seq., 42 U.S.C. 1320(d) et seq., 45 C.F.R. parts 160 and 164).

(B) A covered entity is subject to the provisions of this section if the covered entity does not send a copy of a notice described in subparagraph (A) of this paragraph to the Attorney General within a reasonable time after the Attorney General requests the copy.

(9)(a) A person's violation of a provision of ORS 646A.600 to 646A.628 is an unlawful practice under ORS 646.607.

(b) The rights and remedies available under this section are cumulative and are in addition to any other rights or remedies that are available under law. [2007 c.759 §3; 2015 c.357 §2]