Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Oregon

**Or. Rev. Stat. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626**

S.B. 583 (signed into law July 12, 2007)

Effective October 1, 2007

S.B. 574 (signed into law June 13, 2013)

Effective Sept. 12, 2013

S.B. 601 (signed into law June 10, 2015)

Effective Jan. 1, 2016

S.B. 1551 (signed into law on March 16, 2018)

Effective June 2, 2018

S.B. 684 (signed into law on May 24, 2019)

Effective January 1, 2020

---

**Application.** Any individual or legal entity, whether or not organized to operate at a profit, or a public body as defined in Or. Rev. Stat. § 174.109 (collectively, Entity) that owns, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses PI in the course of the Entity's business, vocation, occupation or volunteer activities. This does not include any person or entity that contracts with the Entity to maintain, store, manage, process or otherwise access PI for the purpose of, or in connection with, providing services to or on behalf of the Entity.

**Security Breach Definition.** Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of PI maintained or possessed by the Entity.

- Does not include an inadvertent acquisition of PI by an Entity or that Entity's employee or agent if the PI 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 PI.

**Notification Obligation.** An Entity to which the statute applies shall give notice of the breach of security to any consumer to whom the PI pertains.

- Notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, or local agencies responsible for law enforcement, the Entity reasonably determines that the breach has not and will not likely result in harm to the individuals whose PI has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for 5 years.

**Notification to Consumer Reporting Agencies.** If an Entity notifies more than 1,000 individuals under this section, the Entity shall notify, without unreasonable delay, all nationwide consumer reporting agencies of the

timing, distribution, and content of the notification. The Entity shall include the police report number, if available, in its notification to the consumer reporting agencies.

**Attorney General Notification.** The entity must provide notice to the Attorney General, either in writing or electronically, if the number of OR residents affected exceeds 250. The Entity shall disclose the breach of security to the Attorney General in the same manner as to consumers.

**Third-Party Data Notification.** Any person that maintains or otherwise possesses PI on behalf of another person shall notify the other person of any breach of security as soon as practicable, but not later than 10 days after discovering the breach of security or having a reason to believe that the breach of security occurred. That person must also notify the Attorney General in writing or electronically if the number of residents affected exceeds 250 or cannot be determined, unless the Entity has already notified the Attorney General.

**Timing of Notification.** The disclosure shall be made in the most expedient manner possible and without unreasonable delay, but not later than 45 days after discovering or receiving notice of the breach. In providing the notice, the Entity shall take reasonable measures necessary to determine sufficient contact information for the individuals, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the PI.

**Personal Information Definition.**

1) An OR resident's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction, or other methods have not rendered the data unusable or if the data elements are encrypted and the encryption key has also been acquired:

- Social Security number;
- Driver's license number or state identification card number issued by the Department of Transportation;
- Passport number or other identification number issued by the United States;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an OR resident's financial account, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account;
- Biometric data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina, or iris, that are used to authenticate the consumer's identity in the course of a financial or other transaction;
- A consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or
- Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.

2) A username or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the username or means of identification.

PI also includes any PI data element or any combination of the PI data elements without with the consumer's first name or first initial and last name if encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable and the data element or combination of data elements would enable an individual to commit identity theft. PI does not include publicly available information, other than a Social Security number, that is lawfully made available to the general public from federal, state or local government records.

**Notice Required.** Notice shall include at a minimum:

- A description of the breach of security in general terms;
- The approximate date of the breach of security;
- The type of PI that was subject to the breach of security;
- Contact information for the person providing the notice;
- Contact information for national consumer reporting agencies; and
- Advice to the individual to report suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission.

Notice may be provided by one of the following methods:

- In writing;
- By telephone, if the Entity contacts the affected consumer directly; or
- Electronically, if the Entity's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

**Credit Monitoring Services.** If an Entity offers credit monitoring or identity theft prevention services without charge, the Entity may not require the affected individual to provide a credit or debit card number or accept another service offered by the Entity for free. If services are offered for a fee, the Entity must separately, distinctly, clearly, and conspicuously disclose in the offer that the person will charge the consumer a fee. The entity must require compliance with these terms from any company offering services on the entity's behalf.

**Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $250,000, that the affected class of individuals to be notified exceeds 350,000, or if the Entity does not have sufficient contact information to provide notice. Substitute notice consists of the following:

- Conspicuous posting of the notice or a link to the notice on the Entity's website, if the Entity maintains a website; and
- Notification to major statewide television and newspaper media.

**Exception: Compliance with Other Laws.**

In each of the following cases, Oregon's notification requirements do not apply, except that any person claiming one of these exemptions and notifying more than 250 Oregon residents must provide a copy of the individual notice and any notice to any primary or functional regulator, to the Oregon Attorney General:

- **Primary Regulator.** Personal information that is subject to, and an Entity that complies with the notification requirements or breach of security procedures that the person's primary or functional federal regulator adopts, promulgates or issues in rules, regulations, procedures, guidelines or guidance.
- **Gramm-Leach-Bliley Act.** An Entity that complies with regulations regarding notification requirements or breach of security procedures that provide greater protection to PI and at least as thorough disclosure requirements promulgated pursuant to Title V of the Gramm-Leach-Bliley Act.
- **HIPAA/HITECH.** An Entity that complies with regulations promulgated under HIPAA or the HITECH Act.
- **More Restrictive State or Federal Law.** An Entity that complies with a state or federal law that provides greater protection to PI and at least as thorough disclosure requirements for a breach of security of PI than that provided by this section.

**Other Key Provisions:**

- **Unlawful Practice.** Violation of the statute is an unlawful practice under ORS 646.607 (Unlawful Trade Practice).
- **Delay for Law Enforcement.** Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and that agency has made a written request that the notification be delayed. The required notification shall be made after that law enforcement agency determines that its disclosure will not compromise the investigation and notifies the Entity in writing.