RCW 19.255.010 Personal information—Notice of security breaches. (1) Any person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

(2) Any person or business that maintains or possesses data that may include personal information that the person or business does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section and except under subsection (5) of this section and RCW 19.255.030, notice may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001;

(c) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) Email notice when the person or business has an email address for the subject persons;

(ii) Conspicuous posting of the notice on the website page of the person or business, if the person or business maintains one; and

(iii) Notification to major statewide media; or

(d)(i) If the breach of the security of the system involves personal information including a user name or password, notice may be provided electronically or by email. The notice must comply with subsections (6), (7), and (8) of this section and must inform the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer;

(ii) However, when the breach of the security of the system involves login credentials of an email account furnished by the person

or business, the person or business may not provide the notification to that email address, but must provide notice using another method described in this subsection (4). The notice must comply with subsections (6), (7), and (8) of this section and must inform the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

(5) A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(6) Any person or business that is required to issue notification pursuant to this section shall meet all of the following requirements:

(a) The notification must be written in plain language; and

(b) The notification must include, at a minimum, the following information:

(i) The name and contact information of the reporting person or business subject to this section;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

(iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and

(iv) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

(7) Any person or business that is required to issue a notification pursuant to this section to more than five hundred Washington residents as a result of a single breach shall notify the attorney general of the breach no more than thirty days after the breach was discovered.

(a) The notice to the attorney general shall include the following information:

(i) The number of Washington consumers affected by the breach, or an estimate if the exact number is not known;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

(iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach;

(iv) A summary of steps taken to contain the breach; and

(v) A single sample copy of the security breach notification, excluding any personally identifiable information.

(b) The notice to the attorney general must be updated if any of the information identified in (a) of this subsection is unknown at the time notice is due.

(8) Notification to affected consumers under this section must be made in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered, unless the delay is at the request of law enforcement as provided in subsection (3) of this section, or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. [2019 c 241 § 2; 2015 c 64 § 2; 2005 c 368 § 2.]

Effective date—2019 c 241: "This act takes effect March 1, 2020." [2019 c 241 § 8.]

Intent—2015 c 64: "The legislature recognizes that data breaches of personal information can compromise financial security and be costly to consumers. The legislature intends to strengthen the data breach notification requirements to better safeguard personal information, prevent identity theft, and ensure that the attorney general receives notification when breaches occur so that appropriate action may be taken to protect consumers. The legislature also intends to provide consumers whose personal information has been jeopardized due to a data breach with the information needed to secure financial accounts and make the necessary reports in a timely manner to minimize harm from identity theft." [2015 c 64 § 1.]

Similar provision: RCW 42.56.590.