# Chapter 19.255 RCW
# PERSONAL INFORMATION—NOTICE OF SECURITY BREACHES

**Sections**



**RCW 19.255.005 Definitions.** The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

(2)(a) "Personal information" means:

(i) An individual's first name or first initial and last name in combination with any one or more of the following data elements:

(A) Social security number;

(B) Driver's license number or Washington identification card number;

(C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account;

(D) Full date of birth;

(E) Private key that is unique to an individual and that is used to authenticate or sign an electronic record;

(F) Student, military, or passport identification number;

(G) Health insurance policy number or health insurance identification number;

(H) 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; or

(I) Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;

(ii) User name or email address in combination with a password or security questions and answers that would permit access to an online account; and

(iii) Any of the data elements or any combination of the data elements described in (a)(i) of this subsection without the consumer's first name or first initial and last name if:

(A) Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and

(B) The data element or combination of data elements would enable a person to commit identity theft against a consumer.

(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.

(3) "Secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person. [2019 c 241 § 1.]

**Effective date—2019 c 241:** See note following RCW 19.255.010.

**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.*

**RCW 19.255.020 Liability of processors, businesses, and vendors.** (1) For purposes of this section:

(a) "Account information" means: (i) The full, unencrypted magnetic stripe of a credit card or debit card; (ii) the full, unencrypted account information contained on an identification device as defined under RCW 19.300.010; or (iii) the unencrypted primary account number on a credit card or debit card or identification device, plus any of the following if not encrypted: Cardholder name, expiration date, or service code.

(b) "Breach" has the same meaning as "breach of the security of the system" in RCW 19.255.010.

(c) "Business" means an individual, partnership, corporation, association, organization, government entity, or any other legal or commercial entity that processes more than six million credit card and debit card transactions annually, and who provides, offers, or sells goods or services to persons who are residents of Washington.

(d) "Credit card" has the same meaning as in RCW 9A.56.280.

(e) "Debit card" has the same meaning as in RCW 9A.56.280 and for the purposes of this section, includes a payroll debit card.

(f) "Encrypted" means enciphered or encoded using standards reasonable for the breached business or processor taking into account the business or processor's size and the number of transactions processed annually.

(g) "Financial institution" has the same meaning as in *RCW 30.22.040.

(h) "Processor" means an individual, partnership, corporation, association, organization, government entity, or any other legal or commercial entity, other than a business as defined under this section, that directly processes or transmits account information for or on behalf of another person as part of a payment processing service.

(i) "Service code" means the three or four digit number in the magnetic stripe or on a credit card or debit card that is used to specify acceptance requirements or to validate the card.

(j) "Vendor" means an individual, partnership, corporation, association, organization, government entity, or any other legal or commercial entity that manufactures and sells software or equipment that is designed to process, transmit, or store account information or that maintains account information that it does not own.

(2) Processors, businesses, and vendors are not liable under this section if (a) the account information was encrypted at the time of the breach, or (b) the processor, business, or vendor was certified compliant with the payment card industry data security standards adopted by the payment card industry security standards council, and in force at the time of the breach. A processor, business, or vendor will be considered compliant, if its payment card industry data security compliance was validated by an annual security assessment, and if this assessment took place no more than one year prior to the time of the breach. For the purposes of this subsection (2), a processor, business, or vendor's security assessment of compliance is nonrevocable. The nonrevocability of a processor, business, or vendor's security assessment of compliance is only for the purpose of determining a processor, business, or vendor's liability under this subsection (2).

(3)(a) If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington as a consequence of the breach, even if the financial institution has not suffered a physical injury in connection with the breach. In any legal action brought pursuant to this subsection, the prevailing party is entitled to recover its reasonable attorneys' fees and costs incurred in connection with the legal action.

(b) A vendor, instead of a processor or business, is liable to a financial institution for the damages described in (a) of this subsection to the extent that the damages were proximately caused by the vendor's negligence and if the claim is not limited or foreclosed by another provision of law or by a contract to which the financial institution is a party.

(4) Nothing in this section may be construed as preventing or foreclosing any entity responsible for handling account information on behalf of a business or processor from being made a party to an action under this section.

(5) Nothing in this section may be construed as preventing or foreclosing a processor, business, or vendor from asserting any

defense otherwise available to it in an action including, but not limited to, defenses of contract, or of contributory or comparative negligence.

(6) In cases to which this section applies, the trier of fact shall determine the percentage of the total fault which is attributable to every entity which was the proximate cause of the claimant's damages.

(7) The remedies under this section are cumulative and do not restrict any other right or remedy otherwise available under law, however a trier of fact may reduce damages awarded to a financial institution by any amount the financial institution recovers from a credit card company in connection with the breach, for costs associated with access card reissuance. [2010 c 151 § 2.]

***Reviser's note:** RCW 30.22.040 was recodified as RCW 30A.22.040 pursuant to 2014 c 37 § 4, effective January 5, 2015.

**Intent—2010 c 151:** "The legislature recognizes that data breaches of credit and debit card information contribute to identity theft and fraud and can be costly to consumers. The legislature also recognizes that when a breach occurs, remedial measures such as reissuance of credit or debit cards affected by the breach can help to reduce the incidence of identity theft and associated costs to consumers. Accordingly, the legislature intends to encourage financial institutions to reissue credit and debit cards to consumers when appropriate, and to permit financial institutions to recoup data breach costs associated with the reissuance from large businesses and card processors who are negligent in maintaining or transmitting card data." [2010 c 151 § 1.]

**Effective date—2010 c 151:** "This act takes effect July 1, 2010." [2010 c 151 § 3.]

**Application—2010 c 151:** "This act applies prospectively only. This act applies to any breach occurring on or after July 1, 2010." [2010 c 151 § 4.]

**RCW 19.255.030 Federal law—Covered entities—Financial institutions.** (1) A covered entity under the federal health insurance portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et seq., is deemed to have complied with the requirements of this chapter with respect to protected health information if it has complied with section 13402 of the federal health information technology for economic and clinical health act, P.L. 111-5 as it existed on July 24, 2015. Covered entities shall notify the attorney general pursuant to RCW 19.255.010(7) in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, P.L. 111-5 as it existed on July 24, 2015, notwithstanding the timeline in RCW 19.255.010(7).

(2) A financial institution under the authority of the office of the comptroller of the currency, the federal deposit insurance corporation, the national credit union administration, or the federal reserve system is deemed to have complied with the requirements of this chapter with respect to "sensitive customer information" as defined in the interagency guidelines establishing information

security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they existed on July 24, 2015, if the financial institution provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response programs for unauthorized access to customer information and customer notice under 12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall notify the attorney general pursuant to RCW 19.255.010 in addition to providing notice to its primary federal regulator. [2019 c 241 § 3.]

**Effective date—2019 c 241:** See note following RCW 19.255.010.

**RCW 19.255.040 Consumer protection.** (1) Any waiver of the provisions of this chapter is contrary to public policy, and is void and unenforceable.

(2) The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this chapter. For actions brought by the attorney general to enforce this chapter, the legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. For actions brought by the attorney general to enforce this chapter, a violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act, chapter 19.86 RCW. An action to enforce this chapter may not be brought under RCW 19.86.090.

(3)(a) Any consumer injured by a violation of this chapter may institute a civil action to recover damages.

(b) Any person or business that violates, proposes to violate, or has violated this chapter may be enjoined.

(c) The rights and remedies available under this chapter are cumulative to each other and to any other rights and remedies available under law. [2019 c 241 § 4.]

**Effective date—2019 c 241:** See note following RCW 19.255.010.