**Revised Code of Washington**
Title 19 – Business Regulations
Chapter 19.255 – Personal Information – Notice of Security Breaches

### § 19.255.010. Disclosure, notice -- Definitions -- Rights, remedies

(1) Any person or business that conducts business in this state and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(2) Any person or business that maintains computerized data that includes personal information that the person or business does not own 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 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, "breach of the security of the system" means unauthorized acquisition of computerized 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.

(5) For purposes of this section, "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 name or the data elements are not encrypted:

(a) Social security number;

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

(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.

(6) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(7) For purposes of this section and except under subsection (8) of this section, "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;* or

(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) E-mail notice when the person or business has an e-mail address for the subject persons;

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

(iii) Notification to major statewide media.

(8) 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.

(9) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.

(10) (a) Any customer injured by a violation of this section may institute a civil action to recover damages.

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

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

(d) A person or business under this section shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.

**§ 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.