2SHB 1149 - H AMD **1114**
By Representative Williams

ADOPTED 02/14/2010

Strike everything after the enacting clause and insert the following:

"NEW SECTION. **Sec. 1.** 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.

NEW SECTION. **Sec. 2.** A new section is added to chapter 19.255 RCW to read as follows:

(1) For purposes of this section:

(a) "Access device" has the same meaning as in RCW 9A.56.010.

(b) "Account information" means: (i) The full, unencrypted magnetic stripe of an access device; (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 an access device or identification device, plus any of the following if not encrypted: Cardholder name, expiration date, or service code.

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

(d) "Business" means an individual, partnership, corporation, association, organization, government entity, or any other legal or commercial entity that processes more than six million access device

transactions annually, and who offers or sells goods or services to persons who are residents of Washington.

(e) "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.

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

(g) "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.

(h) "Service code" means the three or four digit number in the magnetic stripe or on an access device that is used to specify acceptance requirements or to validate the card.

(i) "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.

(2) Processors, businesses, and vendors are not liable under this section if (a) the account information was encrypted during storage and transmittal 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 with payment card industry data security standards, if its compliance was validated on all system components where cardholder data is stored, processed, or transmitted at the time of its last annual security assessment, and if this assessment took place no more than one year prior to the time of the breach.

(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 access devices

that are incurred by the financial institution to mitigate potential current or future damages to its access device account 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.

NEW SECTION. **Sec. 3.** This act takes effect July 1, 2010.

NEW SECTION. **Sec. 4.** This act applies prospectively only. This act applies to any breach occurring on or after the effective date of this section."

1 Correct the title.

EFFECT: The definition of "merchant" is modified by changing the defined word from "merchant" to "business." Definitions of "encrypted," "financial institution," and "vendor" are added. A provision that stated that the business, processor, or vendor is not liable if they comply with any applicable information security standard is modified. The protection from liability now occurs if the business, processor, or vendor has complied with standards adopted by the Payment Card Industry Security Council. Compliance is established if the business, processor, or vendor is completely validated on all components of security at an annual security assessment that occurred within twelve months of a breach of security. A provision that limited damages to all reasonable costs incurred to mitigate any possible damages to account holders is removed. A provision is added that limits damages to only reasonable costs related to the issuance of new access devices to persons who reside in the state. A provision is added that holds the vendor only liable to a financial institution if the claim is not foreclosed by another law or by a contract of the financial institution. A vendor is only liable to the degree that the damages are proximately caused and liability is allowed under law and under contract of the financial institution. A trier of fact may reduce any award by any amount recovered already recovered by a financial institution from a credit card company for the breach. Language and clarifying changes are also made.

--- END ---