S-0303.1

SENATE BILL 5564

State of Washington 61st Legislature 2009 Regular Session

By Senators Kohl-Welles, Holmquist, and Sheldon

Read first time 01/27/09. Referred to Committee on Labor, Commerce & Consumer Protection.

AN ACT Relating to protecting consumers from breaches of security; amending RCW 19.255.010; adding new sections to chapter 19.255 RCW; and providing an effective date.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

Sec. 1. RCW 19.255.010 and 2005 c 368 s 2 are each amended to read as follows:

(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, if a reasonable person would believe that the breach of the security of the system could cause unencrypted data to be acquired by an unauthorized person. The notice must be provided 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.

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

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

(d) "Unencrypted" means that the personal information was not transformed using an algorithm making the information unreadable to anyone except those possessing a key, using standards appropriate for the industry at the time of the breach of the security of the system.

(e) "Card security code" means the three-digit or four-digit value printed on an access device or contained in the microprocessor chip or magnetic stripe of an access device which is used to validate access device information during the authorization process.

(f) "PIN" means a personal identification code that identifies the cardholder.

(g) "PIN verification code number" means the data used to verify cardholder identity when a PIN is used in a transaction.

(h) "Magnetic stripe data" means the data contained in the magnetic stripe of an access device.

(i) "Service provider" means a person or entity that stores, processes, or transmits access device data on behalf of another person or entity.

(2) No person or entity conducting business in Washington that accepts an access device in connection with a transaction may retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to forty-eight hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to forty-eight hours after authorization of the transaction, provided however, a person or entity may retain credit card security code data, PIN verification code numbers, and the full content of magnetic stripe data with the express consent of the customer using the access device.

(3) (a) Whenever there is a breach of the security of the system of a person or entity that has violated subsection (2) of this section, or that person's or entity's service provider, and that breach of the

security of the system compromises five thousand or more unencrypted individual names or account numbers, the breaching person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders including, but not limited to, any cost incurred in connection with:

(i) The cancellation or reissuance of an access device affected by the breach;

(ii) The closing of a deposit, transaction, checking, share draft, or other account affected by the breach and any action to stop payment or block a transaction with respect to the account;

(iii) The opening or reopening of a deposit, transaction, checking, share draft, or other account affected by the breach;

(iv) The notification of account holders affected by the breach;

(v) Credit monitoring services on accounts affected by the breach for a period of one year from the time the issuer of the access device is notified of the breach; and

(vi) Reasonable attorneys' fees and costs associated with the action.

(b) The remedies under (a) of this subsection are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

(4) In an action under this section, a financial institution that provided or approved equipment used to process payment transactions, to a person or entity, is precluded from recovering under this section against the person or entity if the breach of the security of the system was directly related to the equipment provided or approved by the financial institution, and the equipment was being used in the manner recommended by the financial institution.

(5) A person or entity accepting an access device in connection with a transaction may add an additional two cents per transaction to the balance of the transaction for the purpose of subsidizing costs associated with insurance designed to protect against liability associated with the costs referenced in subsection (3) of this section.

NEW SECTION. **Sec. 3.** A new section is added to chapter 19.255 RCW to read as follows:

(1) The parties to a dispute arising under the provisions of this chapter may agree, in writing, to submit to arbitration.

(2) The arbitration process must be administered by any arbitrator agreed upon by the parties at the time the dispute arises if the procedures comply with the requirements of chapter 7.04A RCW relating to arbitration.

(3) Parties to a dispute arising under the provisions of this chapter may seek any remedy provided under subsection (2) of this section or otherwise provided by law and, in addition, a party to a dispute under this chapter entering into arbitration as an initial method of dispute resolution may seek a refund or credit made to an account holder to cover the cost of any unauthorized transaction related to the breach, except that costs under this subsection may not include any amounts recovered by the financial institution from a credit card company.

NEW SECTION. **Sec. 4.** This act takes effect January 1, 2010, providing remedies for a breach of the security of the system occurring after that date.

--- END ---