SENATE BILL REPORT
SB 5564

As Reported by Senate Committee On:
Labor, Commerce & Consumer Protection, February 19, 2009

Title: An act relating to protecting consumers from breaches of security.

Brief Description: Protecting consumers from breaches of security.

Sponsors: Senators Kohl-Welles, Holmquist and Sheldon.

Brief History:
Committee Activity: Labor, Commerce & Consumer Protection: 2/05/09, 2/09/09, 2/19/09 [DPS, DNP].

SENATE COMMITTEE ON LABOR, COMMERCE & CONSUMER PROTECTION

Majority Report: That Substitute Senate Bill No. 5564 be substituted therefor, and the substitute bill do pass.
Signed by Senators Kohl-Welles, Chair; Keiser, Vice Chair; Franklin and Kline.

Minority Report: Do not pass.
Signed by Senators Holmquist, Ranking Minority Member; Honeyford and King.

Staff: Ingrid Mungia (786-7423)

Background: State Security Breach Law (Chapter 19.255 RCW). In 2005 the Legislature enacted a security breach law. The law requires any person or business to notify possibly affected persons when security is breached and unencrypted personal information is (or is reasonably believed to have been) acquired by an unauthorized person. A person or business is not required to disclose a technical breach that does not seem reasonably likely to subject customers to a risk of criminal activity. "Personal information" is defined as an individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted:

- social security number;
- driver's license number or Washington identification card number; or
- 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.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

The notice required must be either written, electronic, or substitute notice. If it is electronic, the notice provided is consistent with federal law provisions regarding electronic records, including consent, record retention, and types of disclosures. Substitute notice is only allowed if the cost of providing direct notice exceeds $250,000; the number of persons to be notified exceeds 500,000; or there is insufficient contact information to reach the customer. Substitute notice consists of all of the following:

- electronic mail (e-mail) notice when the person or business has an e-mail address for the subject persons;
- conspicuous posting of the notice on the website page of the person or business, if the person or business maintains one; and
- notification to major statewide media.

A customer injured by a violation of the security breach law has the right to a civil action for damages.

State Disposal of Personal Information Law. State law places restrictions on how certain types of personal information may be disposed. If a person or business is disposing of records containing personal financial and health information and personal identification numbers issued by a government entity, the person or business must take all reasonable steps to destroy, or arrange the destruction of, the information. An individual injured by the failure of an entity to comply with the disposal of personal information law may sue for:

- $200 or actual damages, whichever is greater, and costs and reasonable attorneys' fees if the failure to comply is due to negligence; or
- $600 or three times actual damages (up to $10,000), whichever is greater, and costs and reasonable attorneys' fees if the failure to comply is willful.

The Attorney General may bring a civil action in the name of the state for damages, injunctive relief, or both, against an entity that fails to comply with the law. The court may award damages that are the same as those awarded to individual plaintiffs.

Summary of Bill: The bill as referred to committee not considered.

Summary of Bill (Recommended Substitute): No person, entity conducting business in Washington, or service provider for such a person or entity that accepts an access device in connection with a transaction may retain the card security code data, the Personal Identification Number (PIN) verification code number, or the full contents of any track of magnetic stripe data after the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after the authorization of the transaction. This does not apply if the person, entity conducting business in Washington, or service provider has the express consent of the customer using the access device.

Remedies. A person or entity must reimburse a financial institution if there is a breach of the security of the system of a person or entity or their service provider and the:

- person or entity or their service provider has violated the card retention provisions in the bill; and

- breach compromises 5,000 or more unencrypted individual names or account numbers during one breach occurrence, or multiple breach occurrences during a one-month period.

The reimbursement is for a financial institution that issued any access devices affected by the breach for all actions reasonably undertaken in order to protect consumers, including costs for:

- the cancellation or reissuance of an access device affected by the breach;
- 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;
- the opening or reopening of a deposit, transaction, checking, share draft, or other account affected by the breach;
- the notification of account holders affected by the breach;
- 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
- reasonable attorneys' fees and costs associated with the action.

The remedies are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

Limited Immunity. A financial institution that provided or approved equipment used to process payment transactions is precluded from recovering cost if:

- the breach of the security of the system is 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.

Additional Transaction Fees Permitted. 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 of a breach.

Arbitration. The parties to a dispute arising under the security breach provisions may agree to submit to arbitration. The arbitrator must be agreed upon by the parties at the time the dispute arises. The arbitration process must comply with the requirements of chapter 7.04A RCW relating to arbitration. A party to a dispute entering into arbitration as an initial method of dispute resolution may seek also a refund or credit made to an account holder to cover the cost of any unauthorized transaction related to the breach, except that costs may not include any amounts recovered by the financial institution from a credit card company. Any other remedy provided by law may also be sought by a party.

Appropriation: None.

Fiscal Note: Available.

Committee/Commission/Task Force Created: No.

Effective Date: The bill takes effect on January 1, 2010.

Staff Summary of Public Testimony: PRO: Washington enacted its security breach law in 2005. Prior to then there were security breaches, although we may not have heard of them because there was no requirement to disclose this information. Currently, if a financial institution accepts a debit or credit card, the financial institution isn't allowed to bring a suit for a security breach. This bill would change that, but sets the threshold high before a financial institution can take any action. There is a high cost associated with taking aggressive steps to combat fraud in the case of a security breach. Some of the smaller institutions have a harder time absorbing the costs which include notifying customers, reissuing cards, closing breached accounts, and taking other measures.

CON: This bill creates strict liability whether or not the retailer was actually liable for the breach. This bill doesn't require any increased security measures to combat breach, just a right of action to sue a retailer if there is a breach. The costs of litigation would be passed onto consumers, which would be a challenge in this tough economy. The industry is already subject to strict penalties in the case of a security breach, so the business would have to pay twice under this bill. One of the challenges is the service providers who process the transactions are out of state, so the financial institutions are not able to go after them, but they want someone to pay for the costs they incur, although interchange fees financial institutions receive are paid, in part, to address this very issue.

Persons Testifying: PRO: Stacy Augistine, Mark Minickiello, Washington Credit Union League; Debie Keesee, Spokane Media Federal Credit Union.

CON: Holly Chisa, Northwest Grocery Association; Michael Transue, Washington Restaurant Association; Mark Johnson, Washington Retail Association; Denny Eliason, Washington Bankers Association.