SENATE BILL REPORT
SHB 2838

As of February 27, 2008

Title: An act relating to personal information associated with debit and credit cards issued by financial institutions.

Brief Description: Regulating retention of personal information associated with access devices.

Sponsors: House Committee on Insurance, Financial Services & Consumer Protection (originally sponsored by Representatives Williams, Roach, Kirby, Simpson, Ericks and Haler).

Brief History: Passed House: 2/15/08, 89-0.
Committee Activity: Financial Institutions & Insurance: 2/26/08.

SENATE COMMITTEE ON FINANCIAL INSTITUTIONS & INSURANCE

Staff: Diane Smith (786-7410)

Background: In 2005 the Legislature enacted a security breach law. This law requires state agencies and private companies to notify possibly affected persons when security is breached and unencrypted personal information is, or could 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.

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 is either direct, written or electronic notice, or substitute notice. Substitute notice includes notification to major statewide media. 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.

A customer injured by a violation of this section has the right to a civil action for damages.

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.

Summary of Bill: Any person or business that is required to disclose a breach of the security of the system is liable to a financial institution for negligence if the breach was comprised of 5,000 or more unencrypted individual names or account numbers.

Unencrypted means that transformation of the personal information did not occur using an algorithm making the information unreadable to anyone except one with a key, using standards appropriate for the industry at the time of the breach. A financial institution may recover for actions reasonably undertaken in order to protect consumers, including costs for: the cancellation or reissuance of an affected access device; the closing, opening, or reopening of any account; any stop payment or block of a transaction; any refund or credit to the cardholder; the notification of the cardholder; credit monitoring services on affected accounts for one year; and reasonable attorneys' fees and costs.

A person or business is not liable to the financial institution if the person or business: met industry standards for the usage and storage of personal information; maintained an internal policy on the treatment of personal information; and consistently provided training to staff on this policy at the time of the data breach.

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.

Appropriation: None.

Fiscal Note: Available.

Committee/Commission/Task Force Created: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony on Substitute Bill: PRO: This is a bi-partisan bill that builds on past work on identity theft and security breach. The burden of identity theft has fallen on financial institutions dealing with panicked customers who want to cancel credit and debit cards. It gives a right of action to the financial institution. The bill has required compromises. Using the $5,000 or more threshold protects the small businesses and the bill really applies to gross negligence in failing to implement basic safeguards. The growth of financial fraud has been astronomical. Personal information is already at risk or compromised. Should financial institutions just notify their customers or should they take aggressive steps to protect them? We are dealing with a loss of consumer confidence. At a conservative $20 per card, the TJ Maxx breach of 94 million records results in $620 million in loss. The bill passed in 2005 was one of the first in the country to protect consumers. There are some misconceptions that need to be cleared up. This bill is about proactive steps to protect consumers. All financial institutions sue in court which is a neutral, impartial venue. Interchange fees do not cover increased fraud costs of financial institutions. The contractual avenue for credit unions is of unequal bargaining power compared to that of large banks. The average credit union has less than $184 million in assets. The kind of fraud losses involved are due to security breaches of over $5,000 lost, unencrypted accounts of personal information as already defined by statute.

CON: This bill is not about the consumer. Consumers are already protected under federal law, by reimbursement of all but $50, which is usually waived. This bill is about business. It gives a special right of action to one party. Retailers pay costs already and financial institutions already are reimbursed. TJ Maxx paid $40 million in fines. This bill hits a mosquito with a sledgehammer and comes back to us for costs. This is not proper public policy. The merchant already has significant fines from VISA.

Persons Testifying: PRO: Representative Williams, prime sponsor; Larry Hoff, Fibre Federal Credit Union; Stacy Augustine, Washington Credit Union League.

CON: Vicky Marin, Washington Retail Association; Denny Eliason, Washington Bankers Association.