SENATE BILL REPORT
SB 6425

As of January 23, 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: Senators Franklin, Benton, Prentice and Rasmussen.

Brief History:
Committee Activity: Financial Institutions & Insurance: 1/22/08.

SENATE COMMITTEE ON FINANCIAL INSTITUTIONS & INSURANCE

Staff: Diane Smith (786-7410)

Background: Lax adherence to security standards by businesses who are custodians of identifying information can contribute to the ease with which identity theft and financial fraud can be committed against their customers. Washington ranks ninth in the nation in per capita identity theft crimes.

When consumer data has been compromised, the business must alert the financial institutions of those consumers affected by the data breach. The financial institution may either notify consumers of a possible risk of fraud or it can take steps to cancel the consumer's plastic cards, change the account numbers, flag the account for increased monitoring, and re-issue any credit or debit cards associated with the account.

Costs to the financial institution are associated with the second option. Estimates of this cost run from the 20 dollar cost to replace the plastic card, to as much as 180 dollars per account when total costs are included. These costs are in addition to any credit given to the consumer for unauthorized purchases related to the data breach.

An organization called the PCI Security Standards Council (Council) was founded in 2006 by the major credit card issuers to continually update standards for the security of account data. The Council's data security standards include requirements for security management, policies, procedures, network architecture, software design, and other protective measures.

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

SUMMARY OF BILL (Proposed Substitute): A right of action is established in favor of the issuer of a credit card, or like device, against any business that owns or licenses computerized data that includes personal information.

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.

The action is for negligence for a breach of the business' data security system if the issuer's costs, resulting from the actions the issuer reasonably undertakes to protect consumers, are more than 5,000 dollars.

If the business met payment card industry data security standards at the time of the data breach, there is a presumption against negligence.

Appropriation: None.

Fiscal Note: Not requested.

Committee/Commission/Task Force Created: No.

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

Staff Summary of Public Testimony: PRO: Credit unions serve 2.4 million customers in Washington. The proposed substitute bill is being heard because of concerns about the initial draft. The 5 thousand dollar threshold was added to ameliorate the effect of the bill on small businesses. It is good public policy to encourage financial institutions to step in and protect consumers. Credit unions do not have direct contracts with the retailers. A little less than 5.5 records per second were stolen last year. Data breach laws require the financial institution to give notice to card-holders. This bill is one more step: it allows recovery of the operational costs of aggressively protecting the customer. Woodstone Credit Union receives four or five notices of data breach per year. Taking the TJ Maxx data breach as an example, 94 million records were lost. If one third of those were customers of the credit union, times the cost of 20 dollars per card to cancel and reissue the cards, the cost would be 620 million dollars. Rather than just notify its customers, as allowed by law, reducing the issue of the cost of taking aggressive action to protect its customers can lead to more protection being provided. The issue is not just retailers' credit card transactions being breached, it is also payroll clerks losing laptops in Starbucks. We are not talking about wholesale data loss. This bill covers casual data losses. All that is required is compliance with reasonable standards to prevent data loss. The principal is simple: your (retailer) carelessness makes you liable. The credit union cannot have a contract with each and every retailer in the state.

CON: Retailers carefully protect customers' data. They do not want to protect bad actors like TJ Maxx. This bill is unnecessary at this time. There already exists a contract between the card-issuer and the retailer. This is where the substance of this bill is appropriately to be placed. The retailer already pays interchange fees of from two to four percent. These fees are, in part, designed to cover costs from a data breach. Why single out retailers? Government agencies like Public Utility Districts, schools, and libraries all have data breach issues. The fiscal note would be astronomical. This is only appropriate for national action; there should not be state action. The proponents of this bill have been very good to work with. We are meeting at noon today to work on the bill. This bill just transfers the costs that federal law required the financial institution to pay, and shifts those costs to the retailer. There is no consumer protection here, beyond what the law already provides. State law already requires the consumer to be made whole. The retailer is the victim of the crime of data breach. The retailer should not be made strictly liable for the crime committed by a third party. The bill does not create a safe harbor since there is no clear release of liability from following the payment card industry (PCI) standards. These standards frequently change and it is not fair

for the small retailer to have to keep up with that. PCI is a trade association for credit card issuers. Five thousand dollars can be exceeded even in a small business that has had one credit card number breached. Credit card issuers should be encouraged to address this problem in their contracts.

Persons Testifying: PRO: Stacy Augustine, Washington Credit Union League; Susan Strifel, Woodstone Credit Union; Gary Gardner, Boeing Employees Credit Union.

CON: Scott Hazelgrove, Washington State Auto Dealer Association; Troy Nichols, National Federation of Independent Business; Mark Johnson, Washington Retail Association.