HOUSE BILL REPORT
HB 2838

As Reported by House Committee On:
Insurance, Financial Services & Consumer Protection

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: Representatives Williams, Roach, Kirby, Simpson, Ericks and Haler.

Brief History:
Committee Activity:
Insurance, Financial Services & Consumer Protection: 1/22/08, 2/5/08 [DPS].

Brief Summary of Substitute Bill

- Provides cause of action for a financial institution against a person or business if there is a breach of security affecting 5,000 or more unencrypted individual names or account numbers.

HOUSE COMMITTEE ON INSURANCE, FINANCIAL SERVICES & CONSUMER PROTECTION

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 8 members: Representatives Kirby, Chair; Kelley, Vice Chair; Roach, Ranking Minority Member; Hurst, Loomis, Rodne, Santos and Smith.

Minority Report: Without recommendation. Signed by 1 member: Representative Simpson.

Staff: Jon Hedegard (786-7127).

Background:

State Security Breach Law (Chapter 19.255 RCW)
In 2005 the Legislature enacted a security breach law. The law requires state agencies and private companies to notify possibly affected persons when security is breached and unencrypted personal information is (or is reasonably believed to have been) acquired by an

---

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.

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.

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.

Additional Federal and State Privacy Protections

Federal and state health privacy laws generally include security provisions and safeguards for health information, including information relating to an individual's identity and payment information. These duties are imposed on health insurers, providers, and others in the health system.

Federal banking and insurance laws generally include security provisions and safeguards for individually identifiable health and financial information. These duties are placed on individuals and businesses in the banking community.

Payment Card Industry Security Standards Council

The Payment Card Industry Security Standards Council (Council) is a limited liability corporation with the mission of enhancing payment account data security by fostering broad adoption of their standards for payment account security. The Council was established by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International in 2004. The Council developed the Payment Card Industry Data Security Standards (PCI DSS). According to the Council, there were six principles and requirements in developing the requirements for security management, policies, procedures, network architecture, software design and other measures:

- build and maintain a secure network;
- protect cardholder data;
- maintain a vulnerability management program;
- implement strong access control measures;
- regularly monitor and test networks; and
- maintain an information security policy.

The Council does not enforce the PCI DSS. Individual payment systems establish contractual terms and penalties for noncompliance.

Summary of Substitute Bill:

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

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 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.

Substitute Bill Compared to Original Bill:

A number of provisions were altered or added to in the substitute bill, including: the 5,000 name or account number threshold for bringing a suit; the "safe harbor" provisions involving industry standards, internal policies, and training; and the provisions regarding equipment provided or approved by a financial institutions.

A number of provisions were removed in the substitute bill, including: the intent section; the requirement that any person or business "promptly" dispose of personal consumer information associated with a credit or debit card; the requirement that businesses meet PCI security standards if they regularly take credit or debit cards; and the provisions that allowed the defendant in a proposed suit to have a suit dismissed quickly if the defendant could prove that they met PCI standards.

Appropriation: None.

Fiscal Note: Available.

Effective Date of Substitute Bill: The bill takes effect 90 days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony:

(In support) The security breach legislation adopted in 2005 had an unintended consequence. The costs associated with the breach were not required to be paid by the negligent actor. People should be liable for their actions that cause harm to others. The bill allows a right of recovery if a person or business fails to meet security standards in retaining and storing information. This is a rather minimal standard. The bill correctly shifts the burden for causing harm to the person who causes the harm. This is good public policy. It supports two important principles. First, this information is important and should be properly encrypted and disposed of at an appropriate time. Second, it allows for a suit against a negligent person. All of the major credit cards utilize these standards. People who accept credit cards today should be following these standards. A financial institution does not have a contract with a retailer and cannot sue them for the costs of a breach under current law. Financial fraud grows annually. Washington was one of the first states to pass a security breach law. If there is a breach, the financial institution must make a decision about what they should do to protect the customer. They could give notice by mail, give notice over the phone, place a fraud warning, put a stop on the card, or cancel the card and issue a new card. There is a cost in all of these actions. Financial institutions then have to decide how much protection to provide and how much cost to absorb. If someone is negligent and it results in a loss, they should have to pay for their negligence.

(Opposed) Retailers do protect the information of their customers. This bill is not needed at this time. It interferes with a contractual relationship between a retailer and a payment system. Codifying a specific standard would reduce flexibility because the Legislature would have to revise the law every time the standard changed. The contracts between a retailer and a payment system are detailed and include penalties for violations. The proponents are planning on working on a proposed substitute bill. That is a step in the right direction.

Persons Testifying: (In support) Representative Williams, prime sponsor; Stacy Augustine, Washington Credit Union League; Susan Streifel, Woodstone Credit Union; and Gary Garcher, Boeing Employees Credit Union.

(Opposed) Mark Johnson, Washington Retail Association.

Persons Signed In To Testify But Not Testifying: None.