Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Insurance, Financial Services & Consumer Protection Committee

HB 2838

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

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

Brief Summary of Bill

- Requires a person or business that accepts an access device and stores or collects personal information to comply with data security standards.
- Requires a person or business that accepts an access device to dispose of personal information within a reasonable time after an authorized transaction.
- Provides cause of action for a financial institution against a person or business if there is a breach of security and the person or business is not in compliance with the provisions for the collection and storage of personal information or the disposal of personal information.

Hearing Date: 1/22/08

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 believe 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 means 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:

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.

- 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 such 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 Bill:

"Access device" is defined as a card or device issued by a financial institution that contains a magnetic stripe, microprocessor chip, radio frequency identification or some other means for storage. It includes a credit card, debit card, and stored value card.

"Financial institution" is defined as a bank, trust company, mutual savings bank, savings and loan association, or credit union authorized to do business and accept deposits in this state under state or federal law.

Existing definitions for breach of the security of the system", "notice" and "personal information" are moved to a new definition section for the chapter.

Collection and Storage of Personal Information
A person or business that accepts an access device and stores or collects personal information must comply with the PCI DSS.

Disposal of Personal Information
A person or business that accepts an access device must dispose of personal information "expeditiously and within a reasonable period of time" after an authorized transaction.

Cause of Action
If there is a breach of security, a financial institution may bring a cause of action against a person or business that is not in compliance with the provisions for the:
- collection and storage of personal information; or
- disposal of personal information.

Prior to bringing a suit, a financial institution must request the person or business to provide an authorized certification or assessment of compliance with the PCI DSS. If the person or business provides proof of compliance within thirty days of the notice, a court must dismiss any suit.

Damages
A financial institution may recover actual damages for a violation, including the costs associated with:
- 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 for a year; and
- reasonable attorneys' fees and costs.

Appropriation: None.

Fiscal Note: Requested on January 21, 2008.

Effective Date: The bill takes effect January 1, 2009.