Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Financial Institutions & Insurance Committee

SSB 6043

Brief Description: Addressing breaches of security that compromise personal information.

Sponsors: Senate Committee on Financial Institutions, Housing & Consumer Protection (originally sponsored by Senators Brandland, Fairley, Benson, Keiser, Schmidt, Spanel, Benton, Franklin, Berkey, Kohl-Welles and Rasmussen).

Brief Summary of Substitute Bill

- Requires agencies, individuals, and businesses owning or licensing computerized data to provide notice with respect to any breach of the security of the computerized data system which results or may have resulted in the unauthorized release of unencrypted personal information.
- Provides that customers injured by a violation of the notice requirements may commence a civil action for damages.
- Excepts from the notice requirements a technical breach which does not seem reasonably likely to subject customers to criminal activity.

Hearing Date: 3/24/05

Staff: CeCe Clynch (786-7168).

Background:

"Identity theft" is defined, by the Federal Trade Commission (FTC), as "someone appropriating your personal information without your knowledge to commit fraud or theft." With 5,654 complaints reported in Washington in 2004, this state is eighth among the states in the per capita reporting of identity theft.

Recently, ChoicePoint, a business which collects and compiles personal and financial information about consumers, reported that it had inadvertently sold personal information relating to almost 145,000 people to a criminal enterprise. As required by laws enacted in California in 2002, the company first disclosed the breach to California residents whose personal information had been included in the sale. California was the only state with laws requiring disclosure of the breach to the affected persons but, at the request of authorities in several other states, ChoicePoint later disclosed that residents in other states, the District of Columbia, and three territories also may

have been affected by the breach of security. More than 3000 of the affected persons were Washingtonians.

At this time, legislation relative to the privacy of personal information and prevention of identity theft is being considered in at least 20 states.

Summary of Bill:

Upon discovery or notification of a breach in the security of a computerized data system, any "agency", person, or business that "owns and licenses" computerized data that includes "personal information" is required to notify Washington residents whose unencrypted personal information may have been accessed in the breach. Any agency, person, or business that maintains *but does not own* computerized data that includes personal information must notify the owner or licensee of the information of the breach.

Definitions.
"Agency" includes "all state agencies and all local agencies. 'State agency' includes every state office, department, division, bureau, board, commission, or other state agency. 'Local agency' includes every county, city, town, municipal corporation, quasi-municipal corporation, or special purpose district, or any office, department, division, bureau, board, commission, or agency thereof, or other local public agency."

"Personal information" means an individual's first name or first initial and last name in combination with any one of the following data elements, when either the name or the data elements are not encrypted: (a) social security number; (b) driver's license number or Washington identification card number; *or* (c) 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.

The phrase "owns or licenses" is not defined in the bill or in the particular California code section which it parallels. In a related section of the California Code, it is stated that the phrase "is intended to include, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates."

Notice Requirements.
Notice of the security breach is to be provided by (a) written notice; or, (b) electronic notice if the electronic notice is consistent with federal rules governing consumer disclosures in global and national commerce.

In certain circumstances, substitute notice will suffice, but only if the agency, person, or business demonstrates that (a) the cost of providing written or electronic notice would exceed $250,000; (b) the affected class of subject persons to be notified exceeds 500,000; *or* (c) it has insufficient contact information. Substitute notice, when permitted, must include email notice if the email address of the person is available, conspicuous posting on the website of the agency, person, or business required to provide the notice, *and* notification to major statewide media.

Unlike the California statute after which this bill is apparently modeled, there is an exception to the disclosure and notification requirements if there has been a technical breach of the security system that does not seem reasonably likely to subject "customers" to a risk of criminal activity.

Any waiver of the notice requirements is considered contrary to public policy and void and unenforceable. Any "customer" injured by a violation of the notice requirements may commence a civil suit for damages, and any "business" that violates, proposes to violate, or has violated the notice provisions may be enjoined.

Appropriation: None.

Fiscal Note: Requested on March 17, 2005.

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