FINAL BILL REPORT
ESHB 1078

C 64 L 15
Synopsis as Enacted

Brief Description: Enhancing the protection of consumer financial information.

Sponsors: House Committee on Technology & Economic Development (originally sponsored by Representatives Hudgins, Morris, Robinson, Kirby, Gregerson, Stanford, Ryu, Magendanz and Pollet; by request of Attorney General).

House Committee on Technology & Economic Development
Senate Committee on Law & Justice
Senate Committee on Ways & Means

Background:

State Security Breach Laws.
In 2005 legislation was enacted creating parallel security breach laws. One set of laws applies to any person or business, and the other set of laws applies to all state and local agencies (agency).

These laws require any person, business, or agency that owns or licenses computerized data that includes personal information to notify possibly affected persons when security of the system is breached and unencrypted personal information is (or is reasonably believed to have been) acquired by an unauthorized person. A person, business, or agency is not required to disclose a technical breach that does not seem reasonably likely to subject customers to a risk of criminal activity.

Definitions.
"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person, business, or agency. Good faith acquisition of personal information by an employee or agent of the business or agency is not a breach of security when the personal information is not used or subject to further unauthorized disclosure.

"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;

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.

- 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.

Non-computerized or encrypted data are exempt.

Notification Requirements.
The notice required when security is breached must be either written, electronic, or substitute notice. If it is electronic, the notice provided must be consistent with federal law regarding electronic records, including consent, record retention, and types of disclosures. 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. Substitute notice consists of all of the following:

- electronic mail (e-mail) notice when the person or business has an e-mail address for the subject persons;
- conspicuous posting of the notice on the website of the person or business, if the person or business maintains one; and
- notification to major statewide media.

There are no specific requirements for the content of the notification.

Disclosure of a breach must be made in the most expedient time possible and without reasonable delay. Delayed disclosure is allowed if disclosure would impede a criminal investigation.

Enforcement.
Any customer injured by a violation of the security breach laws may institute a civil action to recover damages.

Consumer Protection Act.
The Consumer Protection Act (CPA) prohibits unfair methods of competition or unfair or deceptive practices in the conduct of any trade or commerce. The CPA may be enforced by private legal action or through a civil action by the Office of the Attorney General. Any person injured by a violation of the CPA may seek actual damages, costs, and attorneys' fees. The court may triple the amount of damages awarded up to $25,000.

Federal Health Insurance and Accountability Act.
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes nationwide standards for the use, disclosure, storage, and transfer of protected health information. Entities covered by HIPAA must have a patient's authorization to use or disclose health care information, unless there is a specified exception. An entity covered under HIPAA must comply with the Health Technology for Economic and Clinical Health Act (HITECH) notification requirements in cases of a data breach. Under HITECH, entities that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose

unsecured protected health information must, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.

Gramm-Leach Bliley Act.
The Gramm-Leach Bliley Act of 1949 (GLBA) requires financial institutions to give their customers privacy notices that explain the financial institution's information collection and sharing practices. Financial institutions created the Interagency Guidelines, which establish information security standards in cases of a data breach, to comply with GLBA requirements. The Interagency Guidelines state that when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay.

Summary:

Parallel changes are made to the laws governing notice of security breaches for persons, businesses, or agencies.

Definitions.
Protected personal information is no longer limited to computerized and unencrypted data. The term "customer" is replaced with "consumer". "Secured" means encrypted in a manner that meets or exceeds the National Institute of Standards and Technology standard or otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable.

Notification Requirements.
Notice is not required if the breach is not reasonably likely to subject consumers to a risk of harm.

If required, notice must:
- be written and in plain language;
- include the name and contact information of the reporting person, business, or agency;
- list the type of personal information breached; and
- include toll-free telephone numbers to major credit reporting agencies if the breach exposed personal information.

If a breach requires notification to more than 500 Washington residents, the following added notification requirements apply:
- submission of an electronic version of the notification to the Attorney General; and
- provision of the number of consumers affected (or estimate if unknown).

Notification of a breach of personal information to affected consumers must be provided no more than 45 days after the breach was discovered, unless an exception applies.

Enforcement.
The Attorney General may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state for violations of this act by persons or businesses. Only the Office of the Attorney General may bring an action under the CPA. An individual maintains the ability to institute a civil right of action to recover damages.

Exemptions.
Persons, businesses, and agencies covered under the HIPAA and in compliance with the HIPAA notification requirements are exempt from notification requirements. Financial institutions in compliance with notification requirements under the GLBA are also exempt from notification requirements. If more than 500 residents are affected by the breach, persons, businesses, and agencies that qualify for a HIPAA exemption and financial institutions that qualify for the GLBA exemption must report the breach to the Office of the Attorney General.

Votes on Final Passage:

House	97	0
Senate	47	0

Effective: July 24, 2015