HOUSE BILL REPORT
ESHB 1078

As Passed Legislature

Title: An act relating to enhancing the protection of consumer financial information.

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).

Brief History:
Committee Activity:
Technology & Economic Development: 1/21/15, 2/17/15 [DPS].
Floor Activity:
Passed House: 3/4/15, 97-0.
Passed Senate: 4/13/15, 47-0.
Passed Legislature.

Brief Summary of Engrossed Substitute Bill

- Modifies notice requirements for a person, business, or agency to affected persons in cases of a data breach.
- Requires disclosure of a security breach of personal information to be made no later than 45 days after the breach was discovered.
- Makes the failure to notify affected consumers of a security breach a violation of the Consumer Protection Act.

HOUSE COMMITTEE ON TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 13 members: Representatives Morris, Chair; Tarleton, Vice Chair; Smith, Ranking Minority Member; DeBolt, Assistant Ranking Minority Member; Fey, Harmsworth, Hudgins, Magendanz, Nealey, Ryu, Santos, Wylie and Young.

Staff: Kirsten Lee (786-7133).

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.

Background:

State Security Breach Laws.
In 2005 the Legislature enacted 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 or business/agency to notify possibly affected persons when security is breached and unencrypted personal information is (or is reasonably believed 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.

Definitions.
"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.

Non-computerized or encrypted data are exempt.

Notification Requirements.
The notice required must be either written, electronic, or substitute notice. If it is electronic, the notice provided must be consistent with federal law provisions 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 page 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 but not to exceed $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 (GLBA) requires financial institutions to give their customers privacy notices that explain the financial institution's information collection and sharing practices. Under the GLBA, a financial institution follows the requirements of the Interagency Guidelines, which establish information security standards in cases of data breach. 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 of Engrossed Substitute Bill:

Parallel changes are made to the laws governing notice of security breaches for persons, businesses, or agencies, with the exception of the GLBA exemption and application of the CPA. However, the GLBA exemption and the CPA apply only to provisions regarding persons and businesses.

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 (NIST) 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 meet the following minimum requirements:
- is written and in plain language;
- includes the name and contact information of the reporting person or business/ agency;
- lists the type of personal information breached; and
- includes toll-free telephone numbers to major credit reporting agencies if the breach exposed personal information.

If a breach results in 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
- providing 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.
A violation is also a violation of the CPA. 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 are in compliance with the HIPAA notification requirements are exempt from notification requirements. Specific financial institutions and are 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.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) This legislation is aimed at protecting consumers. Notice to consumers is one of the greatest things that can be given to consumers to protect against identity theft. Consumers do not always receive the kind of information they need to take necessary actions. The bill requires notice even when non-computerized data is acquired. There is no reason to treat a consumer's information differently if it is computerized and if the information is taken by an unauthorized person. The bill does not require notice to the Attorney General's Office, which makes it very difficult to track breaches and to know what breaches to be aware of. There is a substitute bill being drafted. Unlike the current law, the substitute bill does not assume that all encryption is up-to-date. That substitute bill presumes that if the encryption is up to the current encryption standard then there is no risk of criminal activity. The idea is to encourage businesses to use strong and up- to date encryption methods. Thirty days versus a 90-day notice makes sense because if you wait until 90 days, then the consumers have not been aware of the breach during that period of time and could not have taken appropriate measures to help themselves. The earlier notice gives consumers the tools to protect themselves and take self-help steps. The bill also requires that other information be provided when notice of a breach is given, including the kind of information that is breached and credit card contact information, so consumers can take certain steps to help themselves. The bill maintains the private right of action and includes a presumed damages provision because consumers may be able to demonstrate that they have been injured by the breach, but cannot show the dollar amount. It is a per se violation under the CPA against the business or person that did not provide the notice, but the bill does not allow a private party to bring an action under the CPA.

(With Concerns) The encryption exception should remain in the law. Technologies that are not necessarily encrypted, but that would provide the same protections should also be included in the bill. There is an exception for persons, businesses and agencies in compliance with HIPPA notification requirements and there should also be an exemption for persons and businesses under the GLBA. There should be a GLBA exemption because when there is a data breach, significant costs are already incurred by a person or business and there is already significant regulation under the GLBA. It would be burdensome to persons and businesses to also have to comply with a similar state law. Additional litigation against banks could result because of the minimum damages allowed in the bill. Over notification is also a concern. When a breach occurs, there needs to be sufficient time to investigate the breach and decide who needs to be notified to ensure over notification does not occur, so notification is not ignored in the future. Thirty days is an appropriate time frame. Also, over notification could be a concern if notice is required for encrypted and unencrypted information.

(Opposed) Removing the encryption standard could subject individual businesses to litigation because the encryption they have may be challenged as insufficient in the future. Losing a clear bright line is problematic in regards to encryption. The same rules should apply both in the public and private sector.

Persons Testifying: (In support) Representative Hudgins, prime sponsor; and Shannon Smith, Office of the Attorney General.

(With concerns) Megan Schrader, TechNet; Denny Eliason, Washington Bankers Association; and Bob Battles, Association of Washington Business.

(Opposed) Mark Johnson, Washington Retail Association; and Scott Hazelgrove, Direct Marketing Association.

Persons Signed In To Testify But Not Testifying: None.