Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Technology & Economic Development Committee

HB 1078

Brief Description: Enhancing the protection of consumer financial information.

Sponsors: Representatives Hudgins, Morris, Robinson, Kirby, Gregerson, Stanford, Ryu, Magendanz and Pollet; by request of Attorney General.

Brief Summary of Bill

- Modifies notice requirements for a person, business, or agency to affected persons in cases of data breach.
- Requires disclosure of a security breach of personal information to be made no later than 30 days after the breach was disclosed.
- Makes the failure to notify affected consumers of a security breach a violation of the Consumer Protection Act.

Hearing Date: 1/21/15

Staff: Kirsten Lee (786-7133).

Background:

State Security Breach Laws (chapter 19.255 RCW and chapter 42.56 RCW).
In 2005 the Legislature enacted parallel security breach laws. Under RCW 19.255.010 the law applies to any person or business. Under RCW 42.56.590, the law 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.

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.

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 is 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 statutes may institute a civil action to recover damages.

Summary of Bill:

Amendments to the current law in this bill apply identically to RCW 19.255.010 and RCW 42.56.590.

Definitions.
Protected personal information is no longer limited to computerized and unencrypted data. The term customer is replaced with consumer throughout the statutes.

Notification Requirements.

Notice is not required if the breach is not reasonably likely to subject consumers to a risk of criminal activity. A technical breach is no longer exempt from disclosure.

If notice is required, there are added requirements for what must be contained in the notice. 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 in the most expedient time possible and without delay is further defined as, "no more than 30 days after the breach was discovered. "

Enforcement.
A violation of this law is also a violation of the Consumer Protection Act (CPA). Washington's CPA declares that "unfair or deceptive acts or practices" occurring in trade are unlawful. The CPA provides that any person who is injured in his or her business or property through such practices may bring a civil action to recover actual damages sustained and costs of the suit, including reasonable attorney's fees. Treble damages may also be awarded in the courts discretion, provided the damage award does not exceed $25,000.

Added Provisions.
Persons, businesses, and agencies covered under the Federal Health Insurance and Accountability Act are considered in compliance with notification requirements under this law if they are in compliance with the Federal Health Information Technology for Economic and Clinical Health Act.

Appropriation: None.

Fiscal Note: Available.

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