Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Innovation, Technology & Economic Development Committee

HB 1071

Brief Description: Protecting personal information.

Sponsors: Representatives Kloba, Dolan, Tarleton, Slatter, Valdez, Ryu, Appleton, Smith, Stanford and Frame; by request of Attorney General.

Brief Summary of Bill

- Expands the definition of "personal information" in the data breach notice laws.
- Modifies data breach notice requirements.

Hearing Date: 1/16/19

Staff: Yelena Baker (786-7301).

Background:

In 2005, parallel data breach notice laws were enacted: one applies to any person or business and the other to all state and local agencies.

These laws require any person, business, or agency that owns or licenses data that includes personal information to provide a data breach notice to Washington resident consumers whose unencrypted personal information is (or is reasonably believed to have been) acquired by an unauthorized person as a result of a data breach.

Any person, business, or agency that maintains, but does not own, data that includes personal information must also notify the owner or licensee of that data of any data breach if the owner's or licensee's personal information is (or is reasonably believed to have been) acquired by an unauthorized person.

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.

Notice is not required if the data breach is not reasonably likely to subject Washington resident consumers to a risk of harm.

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:

- 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.

Data Breach Notice Requirements.

A data breach notice must include the following information:

- the name and the contact information of the reporting person, business or agency;
- a list of the types of personal information that were or are reasonably believed to have been the subject of a data breach; and
- the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

Additionally, if a breach requires notice to more than 500 Washington residents, the reporting person, business, or agency must electronically submit to the Attorney General:

- a sample data breach notice provided to consumers, excluding any personally identifiable information; and
- the number (or an estimate, if the exact number is unknown) of Washington consumers affected by the breach.

Data breach notices must be provided to affected consumers and to the Attorney General no more than 45 days after the breach is discovered.

Delayed notice is allowed if a law enforcement agency determines that the notification would impede a criminal investigation.

Exemptions.

Persons, businesses, and agencies covered under the federal Health Insurance Portability and Accountability Act (HIPAA) and in compliance with the HIPAA notification requirements are exempt from providing consumers with a data breach notice. When more than 500 Washington residents are affected by the breach, the HIPAA-covered entities must provide a data breach notice to the Attorney General in accordance with the HIPPA timeliness requirements. The notice must contain the same information as is required of entities not covered by the HIPPA.

Financial institutions in compliance with information security rules under the federal Gramm-Leach-Bliley Act (GLBA) are also exempt from providing consumers with a data breach notice. When more than 500 Washington residents are affected by the breach, the GLBA-covered entities must provide a data breach notice to the Attorney General in accordance with the same provisions that apply to entities not covered by the GLBA.

Summary of Bill:

The data breach notice requirement is made applicable to persons, business, or agencies that possess data that includes personal information.

Data breach notice must be made to any person, even non-Washington residents, whose unencrypted personal information is (or is reasonably believed to have been) acquired by an unauthorized person.

Definitions.

The definition of "personal information" is modified to mean an individual's first name or first initial and last name in combination with one or more of the following data elements:

- social security number;
- driver's license number or Washington identification card number;
- 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, or any other numbers or information that can be used to access a person's financial resources;
- full date of birth;
- digital signature;
- student, military, or passport identification number;
- health insurance policy number or health insurance identification number;
- any information about a consumer's medical history or mental or physical condition, or about a health care professional's medical diagnosis or treatment of the consumer; or
- biometric data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patters or characteristics that may identify a specific individual.

"Personal information" includes any of the above-listed data elements, alone or in combination, without the consumer's first name or first initial and last name, if encryption has not rendered the data elements unusable and if the data elements would enable a person to commit identity theft against a consumer.

"Personal information" also includes username and email address in combination with a password or security questions and answers that would permit access to an online account.

Data Breach Notice Requirements.

Data breach notice must be provided to affected consumers no more than 30 days after the breach was discovered and must include the following additional information:

- a timeline of when the breach began;

- when the breach was discovered;
- the containment date; and
- all windows of intrusion.

Data breach notice must be provided to the Attorney General no more than 14 days after the breach was discovered and must include the following additional information:

- a list of the types of personal information that were or are reasonably believed to have been the subject of the breach;
- a timeline of when the breach began, when it was discovered, the containment date, and all windows of intrusion; and
- a summary of containment efforts.

If any of the required information is unknown at the time notice is due, the reporting entity must update its notice to the Attorney General.

Exemptions.

Regardless of the number of persons affected by a data breach, entities in compliance with the notification requirements under the federal Health Insurance Portability and Accountability Act and financial institutions in compliance with information security rules under the federal Gramm-Leach-Bliley Act must provide a data breach notice to the Attorney General.

Appropriation: None.

Fiscal Note: Preliminary fiscal note available.

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