HOUSE BILL REPORT
SHB 1071

As Passed Legislature

Title: An act relating to breach of security systems protecting personal information.

Brief Description: Protecting personal information.

Sponsors: House Committee on Innovation, Technology & Economic Development (originally sponsored by Representatives Kloba, Dolan, Tarleton, Slatter, Valdez, Ryu, Appleton, Smith, Stanford and Frame; by request of Attorney General).

Brief History:
Committee Activity:
Innovation, Technology & Economic Development: 1/16/19, 2/6/19 [DPS].
Floor Activity:
Passed House: 3/1/19, 94-0.
Senate Amended.
Passed Senate: 4/15/19, 46-0.
House Concurred.
Passed House: 4/22/19, 96-0.
Passed Legislature.

Brief Summary of Substitute Bill

- Expands the definition of "personal information" in the data breach notice laws.
- Requires certain additional information to be provided in a data breach notice to affected consumers and to the Attorney General.
- Authorizes additional methods of providing a data breach notice to affected consumers.
- Shortens the period of time to provide notice to affected consumers and the Attorney General from 45 days to 30 days.

HOUSE COMMITTEE ON INNOVATION, TECHNOLOGY & ECONOMIC DEVELOPMENT

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.

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives Hudgins, Chair; Kloba, Vice Chair; Smith, Ranking Minority Member; Boehnke, Assistant Ranking Minority Member; Morris, Slatter, Tarleton, Van Werven and Wylie.

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.

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 may be provided by one of the following methods:

- written notice;
- electronic notice in accordance with federal provisions regarding electronic records and signatures; or
- substitute notice consisting of an electronic mail (email) notice, conspicuous website notice, and notification to major statewide media.

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 Substitute Bill:

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 account;
- full date of birth;

- a private key that is unique to an individual and that is used to authenticate or sign an electronic record;
- 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.

If the breach of the security of the system involves personal information that includes a user name or password, data breach notice may be provided electronically or by email. Such notice must inform the person whose personal information has been breached to take certain steps to protect the person's online account. However, when the breach of the security of the system involves login credentials of an email account furnished by a person or business, notification by email to that account is not permitted.

Data breach notice must be provided to affected consumers no more than 30 days after the breach was discovered and must additionally include a time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach. An agency may delay notification to affected consumers for up to an additional 14 days to allow for notification to be translated into the primary language of the affected consumers.

Data breach notice must be provided to the Attorney General no more than 30 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 timeframe of exposure, if known, including the date of the breach and the date of the discovery of the breach; and
- a summary of the steps taken to contain the breach.

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.

Appropriation: None.

Fiscal Note: Available.

Effective Date: The bill takes effect on March 1, 2020.

Staff Summary of Public Testimony:

(In support) It is impossible for consumers to participate in the modern economy without vast amounts of their personal information being collected, transferred, stored, and sold. Data breach and identity theft are significant threats to Washington residents, business, and agencies. This bill strengthens protections for consumers whose data has been compromised by data breaches. According to the Attorney General's report, data breaches affected 3.4 million Washingtonians in 2018, and that applies only to the personal information that currently is required to be disclosed in the event of a data breach. This does not include Washingtonians whose personal information of a different sort was compromised. Other states have expanded their definition of "personal information" to include other categories of data that are now included in this bill. Data breaches often take a long time for the breached entity to discover. Cybercriminals often try to monetize stolen information as quickly as they possibly can, so the more time that passes between a breach and the time a victim is notified, the more damage is done. It is important that consumers have notice of the breach as soon as possible in order to protect their information. This bill also requires accelerated notice to the Office of the Attorney General so that it may take the necessary steps to further protect consumers. The expanded definition of "personal information" includes full date of birth. Washington should follow the example of other states that do not have the "harm trigger" in their data breach laws.

(Opposed) None.

(Other) It is important to protect consumer data, but it is also important to make sure that this legislation can be implemented without some other consequences. The shorter timeframe in which to provide notice to the Attorney General may not give enough time to have meaningful information about the breach. This may require subsequent updated reports and cause confusion. Other states that have adopted data breach laws have a 30-day notification deadline and allow for an extension of that for a good cause. There should be different standards of notification if there is a breach of online account information to allow for a quick notice to affected consumers, so that they could change their passwords more quickly than they would if the formal notification process was followed. The bill limits the definition of "secured" to the National Institute of Standards and Technology; the bill should allow for the use of other security standards. The bill should include language that provides for an affirmative defense to tort claims to businesses in compliance with all security standards. The effective date of the bill should be March 2020 to allow retailers time for compliance with new requirements.

Persons Testifying: (In support) Representative Kloba, prime sponsor; Shannon Smith, Office of the Attorney General; Doug Schadel, AARP Washington; Lucinda Young, Washington Education Association; Rowland Thompson, Allied Daily Newspapers of Washington; and Elise Orlick, WashPIRG.

(Other) Trent House, Washington Bankers Association and United Financial Lobby; Mark Johnson, Washington Retail Association; Bob Battles, Association of Washington Business; and Tom McBride, CompTIA.

Persons Signed In To Testify But Not Testifying: None.