SENATE BILL REPORT
SHB 1071

As of March 21, 2019

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: Passed House: 3/01/19, 94-0.
Committee Activity: Environment, Energy & Technology: 3/20/19.

Brief Summary of Bill

- Expands definition of personal information.
- Requires consumers and the attorney general to be notified no more than 30 days after the discovery of a data breach.
- Amends consumer and attorney general notification requirements.

SENATE COMMITTEE ON ENVIRONMENT, ENERGY & TECHNOLOGY

Staff: Angela Kleis (786-7469)

Background: State Security Breach Laws. Under current law, any person or business that conducts business in Washington and all agencies that own, license, or maintain personal information must meet specified requirements regarding the disclosure of any breach of the security system. Certain federally regulated data sets are exempt from disclosure.

Definition of Personal Information. Personal information means an individual's first name or first initial and last name in combination with any one or more of the following data elements:

- social security number;
- driver's license number or Washington identification card number; or
- information that would permit access to an individual's financial account.

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.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notification Requirements. *Consumer.* The breach notification issued to affected, and possibly affected, consumers by a person, business, or agency must be in plain language and include the following:

- name and contact information of reporting person, business, or agency;
- a list of the type of personal information believed to be subject to the breach; and
- contact information of major credit reporting agencies if the breach exposed personal information.

Attorney General. If more than 500 Washington residents affected by a single breach are required to be notified, the reporting person, business, or agency must also submit to the attorney general a copy of the notification sent to consumers and the general number of affected Washington residents.

In general, consumers and the attorney general must be notified of a data breach in the most expedient time possible, without unreasonable delay, and no more than 45 days after the breach was discovered.

Summary of Bill: Definition of Personal Information. When used in combination with an individual's first name or first initial and last name, the definition of personal information is expanded including:

- full date of birth;
- an individual's unique private key that is used to sign an electronic record;
- student, military, or passport identification number;
- health insurance policy number;
- consumer medical information; and
- an individual's biometric data generated by automatic measurements.

The definition of personal information also includes:

- a combination of username or email address with a password or security questions and answers that would permit access to an online account; and
- any data elements or combination of data elements without the consumer's first name or first initial and last name that meet certain conditions.

Notification Requirements. *Consumer.* In addition to current requirements, notifications to a consumer must include a time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach. Consumers must be notified of a data breach no more than 30 days after the breach was discovered with certain exceptions.

Attorney General. In addition to current requirements, notifications to the attorney general must include:

- a list of the type of personal information believed to have been the subject of a breach;
- a time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach;
- a summary of steps taken to contain the breach; and

- a sample copy of the security breach notification.

The attorney general must be notified of a data breach no more than 30 days after the discovery of a data breach. The notice must be updated if any required information is unknown at the time notice is due.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: No.

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

Staff Summary of Public Testimony: PRO: Data breaches are a significant, growing threat to Washington residents. Consumers have the right to know when a data breach has occurred as soon as possible. Overall, Washington residents feel their data is less secure but they are not taking the necessary steps to protect their data. This bill will strengthen consumer protections.

OTHER: We prefer federal regulation. The notification deadlines of 35 days to consumers and 25 days to the attorney general are more appropriate. Date of birth should not be included in the definition of personal information. Alternative notification options should be added in order to address instances where the data breach included email account credentials.

Persons Testifying: PRO: Representative Shelley Kloba, Prime Sponsor; Emilia Jones, Attorney General's Office; Joanna Grist, AARP.

OTHER: Mark Johnson, Washington Retail; Mike Hoover, TechNet; Bob Battles, Association of Washington Business.

Persons Signed In To Testify But Not Testifying: No one.