SENATE BILL REPORT
SB 5064

As of February 18, 2019

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

Brief Description: Protecting personal information.

Sponsors: Senators Nguyen, Darneille, Hasegawa, Wellman, Keiser, Zeiger, Kuderer and Saldaña; by request of Attorney General.

Brief History:
Committee Activity: Environment, Energy & Technology: 1/22/19, 2/07/19 [DPS-TRAN]. Transportation: 2/19/19.

Brief Summary of First Substitute Bill

- Expands definition of personal information.
- Requires the attorney general to be notified no more than 25 days after the discovery of a data breach.
- Requires consumers to be notified no more than 35 days, with certain exceptions, after the discovery of a data breach.
- Amends consumer and attorney general notification requirements.

SENATE COMMITTEE ON ENVIRONMENT, ENERGY & TECHNOLOGY

Majority Report: That Substitute Senate Bill No. 5064 be substituted therefor, and the substitute bill do pass and be referred to Committee on Transportation.

Signed by Senators Carlyle, Chair; Palumbo, Vice Chair; Ericksen, Ranking Member; Fortunato, Assistant Ranking Member, Environment; Billig, Brown, Das, Hobbs, Liias, McCoy, Nguyen, Rivers, Short and Wellman.

Staff: Angela Kleis (786-7469)

SENATE COMMITTEE ON TRANSPORTATION

Staff: Kim Johnson (786-7472)

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. 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.

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. 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.

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.

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

Summary of Bill (First Substitute): 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 to include the following data elements:

- 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 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. 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 35 days after the breach was discovered with certain exceptions.

Notifications to the attorney general must include the following:

- 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 25 days after the breach was discovered. The notice must be updated if any required information is unknown at the time notice is due.

EFFECT OF CHANGES MADE BY ENVIRONMENT, ENERGY & TECHNOLOGY COMMITTEE (First Substitute):

- Requires notification to the attorney general within 25 days rather than 14 days after discovery of a breach.
- Requires notification to a consumer within 35 days rather than 30 days after discovery of a breach.
- Allow companies to comply for password breaches by giving consumers password reset procedures.
- Restores language regarding alternative notice.
- Makes technical corrections.

Appropriation: None.

Fiscal Note: Available.

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

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony on Proposed Substitute (Environment, Energy & Technology): *The committee recommended a different version of the bill than what was heard.* PRO: Dealing with the aftermath of a breach can be a frustrating experience for consumers. We trust our most personal information to these companies and it deserves to be treated with dignity and respect. The current definition of personal information is too narrow to effectively protect consumers in today's environment. A recent study showed most security breaches are not discovered until after 100 days of the breach. The number of days after a breach needs to be shortened in order to allow consumers to take the necessary steps to protect themselves. We think these protections should be extended to public employees if employers are breached.

OTHER: We think the notification timelines included in the bill are too short and do not provide businesses enough time to complete the complex analyses. An effective date of March 2020 would be more appropriate in order to allow for implementation outside of the holiday season. We have concerns with the use of full date of birth as a separate data element when associated with a name set because inclusion might expand the number of groups regulated by this act. We think the bill could be improved by adding a safe harbor for our mutual defense; aligning notification format with current cybersecurity practices; and adding options for referencing other industry-accepted standards.

Persons Testifying (Environment, Energy & Technology): PRO: Senator Joe Nguyen, Prime Sponsor; Lucinda Young, Washington Education Association; Shannon Smith, Attorney General's Office.

OTHER: Trent House, Washington Bankers Association and United Financial Lobby; Mark Johnson, Washington Retail Association; Tom McBride, CompTIA; Bob Battles, Association of Washington Business; Rowland Thompson, Allied Daily Newspapers of Washington.

Persons Signed In To Testify But Not Testifying (Environment, Energy & Technology): No one.