## SB 684 A STAFF MEASURE SUMMARY

**Carrier:** Sen. Prozanski

**Senate Committee On Judiciary**

| | |
|---|---|
| **Action Date:** | 03/27/19 |
| **Action:** | Do pass with amendments. (Printed A-Eng.) |
| **Vote:** | 7-0-0-0 |
| **Yeas:** | 7 - Bentz, Fagan, Gelser, Linthicum, Manning Jr, Prozanski, Thatcher |
| **Fiscal:** | Has minimal fiscal impact |
| **Revenue:** | No revenue impact |
| **Prepared By:** | Channa Newell, Counsel |
| **Meeting Dates:** | 2/26, 3/27 |

**WHAT THE MEASURE DOES:**

Modifies Oregon Consumer Identity Theft Protection Act. Details process for notification to consumer when a consumer's data that is held by a third party vendor is subject to a breach. Requires a vendor to notify the covered entity as soon as practicable, but no more than ten days after discovering a breach or having reason to believe a breach occurred. Requires vendor to notify the Attorney General if breach involved the personal information of more than 250 customers or an undetermined number of customers. Includes username or other means of identifying a consumer for purpose of accessing the consumer account, combined with other authentication factors, as personal information covered by Act. Specifies that entity that is in compliance with Gramm-Leach-Bliley Act (GLBA) or Health Insurance Portability and Accountability Act (HIPAA) for information that is subject to regulation by those Acts need not provide notice as outlined in the measure. Provides affirmative defense to an allegation that entity did not provide notification or security safeguards required by measure to personal information covered by state law, but not federal law, if the entity shows compliance with federal safeguards and notification, even though such is not required of that personal data. Renames Act to Oregon Consumer Information Protection Act. Defines vendor and covered entity. Updates security and safeguard regulations.

**ISSUES DISCUSSED:**

- Consequences of Equifax data breach
- 2018 interim work group
- Provisions of notification by entity with data covered by federal law or state law
- Process for notification of breach by third party vendor

**EFFECT OF AMENDMENT:**

Makes technical corrections. Provides that entity holding data covered by data and security requirements of federal laws are exempt from notification and security requirements of measure. Provides affirmative defense to an allegation that entity did not provide notification or security safeguards required by measure to personal information covered by state law, but not federal law, if the entity shows compliance with federal safeguards and notification, even though such is not required of that personal data.

**BACKGROUND:**

In 2017, a single data breach exposed the names, social security numbers, dates of birth, and in some cases, driver license numbers of 143 million Americans, with 209,000 individuals having their credit card numbers stolen. In response to that breach, a work group was formed to begin revising and updating Oregon's Consumer Identity Theft Protection Act. Senate Bill 1551 was the initial result of that effort, which reconvened in the 2018 interim to further update the Consumer Identity Theft Protection Act.

Senate Bill 684 A is the product of that work group. It provides a mechanism for third-party vendors, such as data storage companies, to notify covered entities when a breach of personal information has occurred. In addition to providing notice to the covered entity, the vendor is also required to give notice to the Attorney General when the breach is of either an undetermined number of consumers, or over 250. Additionally, the measure updates what information is considered protected information so that it includes a user name or other identifier, in combination with other methods of authenticating an account or identifying a consumer. The measure also updates the notice provisions relating to HIPAA and GLBA covered entities, specifying that an entity who is in compliance with federal law for federally covered data need not provide notice under Oregon law, but provides an affirmative defense to those entities for data not covered by federal law, so long as the entity uses the same standards set by federal law in handling the non-covered information.