

HB 4147 A STAFF MEASURE SUMMARY

House Committee On Business and Labor

Action Date: 02/14/18

Action: Without recommendation as to passage, with amendments, and be referred to Rules.
(Printed A-Eng.)

Vote: 6-5-0-0

Yeas: 6 - Bynum, Doherty, Evans, Fahey, Holvey, Piluso

Nays: 5 - Barreto, Boles, Heard, Kennemer, Wilson

Fiscal: Has minimal fiscal impact

Revenue: No revenue impact

Prepared By: Jan Nordlund, LPRO Analyst

WHAT THE MEASURE DOES:

Prohibits consumer reporting agency from charging consumer a fee to place, remove or temporarily lift a security freeze. Expands who must provide notification when security breach occurs to include person who has control over, or access to, personal information. Requires notice of data breach be made in most expeditious manner and that it be made within 45 days of discovering or receiving notice of the breach. Establishes requirements when offering free credit monitoring services or identity theft prevention and mitigation services to a consumer who has been notified of a security breach. Modifies standards for safeguarding personal information. Extends duties to safeguard personal information to those who have control over, or access to, personal information. Provides right of private action under Unlawful Trade Practices Act for violations of identity theft protection statutes. Expands definition of personal information. Takes effect 91 days following adjournment sine die.

ISSUES DISCUSSED:

- Experience of victims of identity theft
- Other states that prohibit charging consumers to place a security freeze
- Standards set by payment networks
- Cost of compliance for businesses
- Whether a consumer will receive multiple notices regarding a single data breach
- Whether those who hold personal information take safeguards seriously
- Whether arbitration clauses will prevent consumers from filing action in court

EFFECT OF AMENDMENT:

Replaces original measure.

BACKGROUND:

Major data breaches involving loss of consumer personal information in the recent past include Home Depot (50 million consumers), Target (412 million consumers), Yahoo (3 billion users), and Equifax (143 million consumers). Cybercriminals who obtain personal information such as name, address, date of birth, or Social Security number are able to open accounts, receive goods and services, and apply for financing under the stolen identity.

Oregon enacted identity theft prevention laws in 2007. When a data breach occurs, Oregon statutes require notice be given to affected consumers; if more than 250 consumers are affected, notice must also be given to the Attorney General. The statutes also require personal information be safeguarded by those who own, maintain, or possess such

HB 4147 A STAFF MEASURE SUMMARY

information. Consumers have the right to protect their information by requesting the consumer reporting agencies freeze access to their consumer report. Under Oregon statutes, consumer reporting agencies are limited to charging no more than \$10 for placing or removing a security freeze. Victims of identity theft may not be charged a fee. Several states have prohibited the consumer reporting agencies from charging any fees to consumers who freezing access to their information.