H-0527.1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**HOUSE BILL 1469**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**State of Washington 64th Legislature 2015 Regular Session**

**By** Representatives Hudgins, Magendanz, Stanford, Ormsby, and Tarleton

AN ACT Relating to the removal of payment credentials and other sensitive data from state data networks; and adding a new section to chapter 43.41A RCW.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec.**  A new section is added to chapter 43.41A RCW to read as follows:

(1) State agencies shall not hold cardholder data or other payment credentials on state data systems.

(2) If payment credentials collected by state agencies are required to be held, these data may be transferred to and stored with a third-party institution that is fully compliant with security standards adopted by the PCI security standards council and certified as such.

(3) If a data security breach resulting in the compromise of payment credentials collected by the state occurs at a third-party institution, and if that institution is found not to have been fully compliant with PCI security standards at the time of the breach, that institution shall be fully financially liable for the damages resulting from the breach. Damages may include costs of notification, credit monitoring, identity theft prevention measures, or any other remedies provided under relevant data breach laws.

(4) State agencies that currently hold payment credentials must work with the office to eliminate these data from state data systems by July 1, 2018.

(5) The office may grant a waiver to the requirement under subsection (4) of this section in instances where transitioning payment credentials off state data systems presents special difficulty, or where holding payment credentials on state data systems is required for the day-to-day business of the agency or by law.

(6) Payment credentials held on state data systems as the result of a waiver granted under subsection (5) of this section shall be transferred to a single, unified and secure data storage system administered by consolidated technology services. This transfer shall be completed by July 1, 2018, unless a secondary waiver extending the deadline is granted by the office.

(7) The office shall develop a policy for removing social security numbers and other sensitive, personally identifiable information from state data systems, with the objective of minimizing storage of these data wherever not required for the day-to-day operations of an agency or by federal law. The policy must include instructions for identifying and classifying sensitive data, removing them where possible, and protecting them as necessary. All state agencies shall comply with this policy.

**--- END ---**