

HOUSE BILL REPORT

HB 1840

As Reported by House Committee On:
Innovation, Technology & Economic Development

Title: An act relating to the removal of payment credentials and other sensitive data from state data networks.

Brief Description: Concerning the removal of payment credentials and other sensitive data from state data networks.

Sponsors: Representatives Smith, Hudgins and Tarleton.

Brief History:

Committee Activity:

Innovation, Technology & Economic Development: 2/13/19, 2/15/19 [DP].

Brief Summary of Bill

- Prohibits state agencies from storing payment credentials on state data systems, except under certain circumstances.
- Prohibits third parties from transferring, selling, monetizing, or otherwise sharing any payment credential data stored for agencies.
- Requires the Office of the Chief Information Officer to develop a policy, to be followed by all agencies, to minimize agency retention of personally identifiable information.

HOUSE COMMITTEE ON INNOVATION, TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: Do pass. Signed by 8 members: Representatives Hudgins, Chair; Kloba, Vice Chair; Smith, Ranking Minority Member; Boehnke, Assistant Ranking Minority Member; Slatter, Tarleton, Van Werven and Wylie.

Staff: Yelena Baker (786-7301).

Background:

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.

In its 2018 Data Breach Report, the Office of the Attorney General stated that data breaches, such as malicious cyberattacks, unintentional breaches, and unauthorized access, compromised the personal information of 3.4 million Washingtonians. Financial information was the most commonly compromised type of data for the third straight year.

The Consolidated Technology Services agency, also known as WaTech, establishes security standards and policies to ensure the confidentiality and integrity of information transacted, stored, or processed in the state's information technology (IT) systems and infrastructure. Each state agency must develop an IT security program.

Within WaTech, the Office of the Chief Information Officer (OCIO) has certain primary duties related to state government IT. The Office of Privacy and Data Protection is housed within the OCIO and serves as a central point of contact for state agencies on policy matters involving data privacy and data protection.

Summary of Bill:

State agencies are prohibited from storing payment credentials on state data systems.

"Payment credentials" include the following:

- the full magnetic stripe or primary account number of a credit or debit card combined with cardholder name, expiration date, or service code; or
- other personally identifiable credentials allowing the state to receive incoming payments for services, excluding account information required for making outgoing payments, distributions, and transfers.

State agencies must work with the Office of the Chief Information Officer (OCIO) to eliminate these data from state data systems by July 1, 2021. The OCIO may grant waivers if 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.

Payment credentials must be stored by third-party institutions which must be fully compliant with industry-leading security standards. If a third-party institution is found not fully compliant with security standards and a security breach occurs, the institution will be fully financially liable for the damages resulting from the unauthorized acquisition of payment credentials as a result of the breach.

Third-party institutions storing payment credential data are prohibited from transferring, selling, trading, monetizing, or otherwise sharing any stored data, unless required by law.

The OCIO must develop a policy, to be followed by all agencies, to minimize the retention of sensitive, personally identifiable information whenever not required for day-to-day operations or by law.

Appropriation: None.

Fiscal Note: Preliminary fiscal note available.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.

Staff Summary of Public Testimony:

(In support) This is a straightforward bill regarding not storing payment credentials state agencies do not need and moving that data to third parties. To help protect that data, third parties are prohibited from sharing the payment credential data they store on behalf of agencies.

(Opposed) None.

Persons Testifying: Representative Smith, prime sponsor.

Persons Signed In To Testify But Not Testifying: None.