AN ACT Relating to the removal of payment credentials and other sensitive data from state data networks; and adding a new section to chapter 43.105 RCW.

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

NEW SECTION. Sec. 1. A new section is added to chapter 43.105 RCW to read as follows:

(1) State agencies shall not store payment credentials on state data systems. For the purposes of this section, "payment credentials" means:

(a) The full magnetic stripe or primary account number of a credit or debit card combined with cardholder name, expiration date, or service code; or

(b) Other personally identifiable credentials allowing the state to receive incoming payments for services, excluding account information required for making outgoing payments, distributions, and transfers.

(2) Payment credentials collected on behalf of a state agency in order to process payments for the agency must be accepted and stored by a third-party institution that is fully compliant with industry leading security standards. A third-party institution is prohibited from transferring, selling, trading, monetizing, or otherwise sharing
any data that is stored pursuant to this section, unless required by law.

(3) If a security incident results in the unauthorized acquisition of payment credentials collected and processed by a third-party institution on behalf of a state agency, and if that institution is found not to have been fully compliant with industry leading security standards at the time of the breach, that institution is 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 store payment credentials must work with the office to eliminate these data from state data systems by July 1, 2021.

(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) The office shall develop a policy for minimizing the retention of social security numbers and other sensitive, personally identifiable information by state agencies whenever not required for the day-to-day operations of an agency or by law. This policy must include instructions for identifying and classifying sensitive data, eliminating it where possible, and protecting them as necessary. The policy must include an examination of the reasons sensitive data are being collected, and any ongoing retention must be justified. All state agencies must comply with this policy.