BILL ANALYSIS

H.B. 1743
By: Guerra
State Affairs
Committee Report (Unamended)

BACKGROUND AND PURPOSE

Vertafore, a software company under contract with the Department of Public Safety, exposed personal information of 27.7 million Texans through a data breach in March of 2020. The data exposed included driver's license numbers, addresses, dates of birth, and vehicle registration history. The breach occurred after three data files were stored in an unsecured external storage device. Texans must be able to trust their state agencies to protect their data, and that trust must extend to contractors that work with the state. H.B. 1743 seeks to ensure this public trust by establishing standards for contractors purchasing state agency data that includes sensitive personal or confidential information or information whose disclosure is otherwise regulated by law and providing penalties for contractors that violate those standards, including temporary debarment from state contracting.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

H.B. 1743 amends the Government Code to restrict the sale of computerized data owned, licensed, or maintained by an applicable state agency to a contractor if the data includes certain sensitive personal or confidential information or information whose disclosure is otherwise regulated by law. The sale of any such data must be authorized under law and the sale contract must include a statement that the contractor will do the following:

- comply with applicable Identity Theft Enforcement and Protection Act notification requirements following a security breach;
- notify the state agency not later than 48 hours after the discovery of the breach of system security, suspected breach of system security, or unauthorized exposure;
- assist each person whose personal information was exposed with protecting the person from identity theft and protecting or restoring the person's credit rating; and
- pay any civil penalty assessed against the contractor.

That statement must also indicate that the contractor acknowledges that its failure to comply with those conditions constitutes a default of the contract on notice from the state agency and may subject them to debarment from state contracting.

H.B. 1743 requires a state agency that determines a contractor is noncompliant with the aforementioned contract standards to refer the matter to the comptroller of public accounts for action. The bill requires the comptroller to bar the contractor from state contracting using the

procedures prescribed by applicable state law and establishes that the debarment expires on the third anniversary of the debarment date. The bill makes a contractor who obtains computerized data that includes information to which the bill applies from a state agency liable to the state for a civil penalty imposed in accordance with applicable provisions of the Identity Theft Enforcement and Protection Act for a breach of system security or an unauthorized exposure of that information.

EFFECTIVE DATE

September 1, 2021.