BILL ANALYSIS

C.S.H.B. 4390
By: Capriglione
Business & Industry
Committee Report (Substituted)

BACKGROUND AND PURPOSE

It has been suggested that regulating the protection by a business of computerized data that includes sensitive personal information may help protect individuals and communities from potential harm resulting from the misuse of such data. C.S.H.B. 4390 seeks to address this issue by strengthening notification requirements in case of a system security breach that involves sensitive personal information and establishing the interim Texas Privacy Protection Advisory Council to study relevant data privacy laws in other states and countries.

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

C.S.H.B. 4390 amends the Business & Commerce Code to change the time by which a person who conducts business in Texas and who owns or licenses computerized data that includes sensitive personal information is required to disclose any breach of system security after discovering or receiving notification of the breach to any individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person from as quickly as possible to without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, subject to certain exceptions. The bill requires a person who is required to disclose or provide notification of a breach of system security under certain provisions of the Identity Theft Enforcement and Protection Act to notify the attorney general of such a breach that involves at least 250 Texas residents and sets out the required contents of that notification.

C.S.H.B. 4390 creates the Texas Privacy Protection Advisory Council and provides for the council's composition, designation of co-chairs, and manner of convening. The bill requires the council to study and evaluate the laws in Texas, other states, and relevant foreign jurisdictions that govern the privacy and protection of information that alone or in conjunction with other information identifies or is linked or reasonably linkable to a specific individual, technological device, or household and to make recommendations to the legislature on specific statutory changes regarding the privacy and protection of that information that appear necessary from the results of the council's study. The bill requires the council, not later than December 1, 2020, to report its findings and recommendations to the legislature and requires the applicable authorities to appoint the members of the council not later than the 60th day after the bill's effective date. The bill establishes that the council is abolished and its provisions relating to the council expire December 31, 2020.

EFFECTIVE DATE

September 1, 2019.

COMPARISON OF ORIGINAL AND SUBSTITUTE

While C.S.H.B. 4390 may differ from the original in minor or nonsubstantive ways, the following summarizes the substantial differences between the introduced and committee substitute versions of the bill.

The substitute includes provisions setting a specific deadline by which a person who conducts business in Texas and owns or licenses computerized data that includes sensitive personal information is required to disclose any breach of system security to an affected individual, requiring additional notification of the attorney general for certain system security breaches, and creating the Texas Privacy Protection Advisory Council.

The substitute does not include any provisions from the introduced version, which provides for requirements for applicable businesses to implement certain risk assessment and security practices and inform individual customers and the public regarding their data collection and processing practices and imposes a civil penalty.