SUBJECT: State and local government notification of a breach of computer security

COMMITTEE: State Affairs — committee substitute recommended

VOTE: 15 ayes — Solomons, Menendez, Cook, Craddick, Farabee, Gallego, Geren, Harless, Hilderbran, Jones, Lucio, Maldonado, Oliveira, Swinford, S. Turner

0 nays

WITNESSES: (*On original version*:)
For — (*Registered, but did not testify*: Brynne Vanhettinga, American Civil Liberties Union of Texas)

Against — None

On — (*Registered, but did not testify*: Ginger Salone, Texas Department of Information Resources)

BACKGROUND: Under Business and Commerce Code, sec. 521.053, if sensitive personal information was, or is believed to have been, acquired by an unauthorized person during a breach of system security, the breach must be disclosed to the owner of that information by a person who conducts business in this state and owns or licenses computerized data that contains sensitive personal information and any person who maintains computerized data that includes sensitive personal information the person does not own.

Disclosure must be made as quickly as possible after discovering the breach, but may be delayed at the request of a law enforcement agency that determines the notification will impede a criminal investigation, until the agency determines the notification will not compromise the investigation.

Disclosure may be made in writing or electronically. If the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person has insufficient contact information, notice may be given by electronic mail, conspicuous posting on the person's website, or notice published in or broadcast on major statewide media.

"Sensitive personal information" means an individual's first name or initial and last name in combination with any one or more of the following, if the name and items are not encrypted:

- social security number;
- driver's license number or government-issued identification number; or
- account, credit, or debit card number in combination with any required password, or security or access code that would permit access to an individual's financial account.

"Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person.

DIGEST:

CSHB 2004 would require a state agency or local government that owned, licensed, or maintained computerized data that included sensitive personal information to comply with the disclosure requirements of Business and Commerce Code, sec. 521.053.

The bill would amend the definition of sensitive personal information to include information that identified an individual and related to that individuals' physical or mental health or condition, the provision of or payment for health care to the individual, or the information in the current definition.

The definition of "breach of system security" would be amended to include encrypted data, if the person accessing the data had the key required for decryption.

The bill would take effect September 1, 2009, and would apply only to breaches of system security that occurred on or after that date.

SUPPORTERS SAY:

By requiring state and local government entities to disclose a security breach, CSHB 2004 would give individuals whose sensitive personal information had been or may have been accessed the opportunity to mitigate damage. Unauthorized access to personal information, such as social security or bank account numbers, could lead to identity theft.

Extending the disclosure requirement to state and local government entities would be a sensible step, given that people often are required by

law to disclose sensitive personal information to government entities in instances such as filing taxes or receiving social services. As collection of this data grows, so does the risk that confidential information will be stolen, misappropriated, or accidentally exposed. Several state agencies, including the Attorney General's Office and the Department of Information Resources, already have a policy of informing affected individuals of any breach of their personal data, and CSHB 2004 would make this policy uniform for all state and local government entities.

OPPONENTS SAY:

No apparent opposition.

NOTES:

CSHB 2004 differs from the bill as filed by adding provisions to Business and Commerce Code, ch. 521 that would amend the definitions of "sensitive personal information" and "breach of system security." The substitute removed a provision that would have added Government Code, ch. 2061, which would provide the mechanism by which a state or local governmental entity would provide notification of a breach of system security, and define "breach of system security," "local government," "sensitive personal information," and "state agency." Instead, the substitute added provisions to Government Code, ch. 2054 and Local Government Code, ch. 205 that would require state and local government entities to comply with the notification requirements set out in Business and Commerce Code, sec. 521.053, and that reference Business and Commerce Code definitions of "breach of system security" and "sensitive personal information."

The companion bill, SB 1884 by Ellis, was reported favorably, as substituted, by the Senate Government Organization Committee on April 23 and recommended for the Local and Uncontested Calendar.