

February 5, 2018

Chairman Mike Stevens
State Capitol
500 E. Capitol Ave
Pierre, SD 57501
Mike.Stevens@sdlegislature.gov

Re: Senate Bill No. 62 (Data Breach)

Dear Chairman Stevens:

The Electronic Transactions Association (“ETA”) opposes the SB 62 because it represents an additional hurdle in building a national uniform data breach notification framework. If enacted, SB 62 would likely increase costs to small businesses that are victims of data breaches. ETA and its members are dedicated to working with federal and state regulators to address the important and growing issue of data security and data breach notification. ETA agrees that delivery of proper notification to affected individuals when data is compromised is vitally important for both businesses and consumers. However, this bill, as written, is not the best vehicle in which to address data breach notification and ETA opposes SB 62. ETA does have some recommendations for language that could help make the bill more uniform.

ETA is the leading trade association for the payments industry, representing more than 500 companies worldwide involved in electronic transaction processing products and services. The purpose of ETA is to influence, monitor, and shape the payments industry by providing leadership through education, advocacy, and the exchange of information. ETA’s membership spans the breadth of the payments industry, and includes financial institutions, payment processors, independent sales organizations, and equipment suppliers. ETA’s members use data to provide a wide range of products and services designed to enhance and secure electronic transfers. Our members rely on data to help reduce fraud and to authenticate transactions to make transactions between businesses and consumers seamless and secure.

GENERAL COMMENTS ON DATA BREACH NOTIFICATION

ETA Supports a National Uniform Data Breach Notification Standard

Consumers and businesses are best served when they have a common and consistent expectation of breach procedures, and company time and resources can be devoted to innovative security solutions to protect against new threats. However, to build the most meaningful and effective data breach solution, it is imperative to tackle this issue with a clear federal standard rather than a patchwork of state laws. Currently, disparate laws in 48 states plus District of Columbia, Guam, Puerto Rico, and the Virgin Islands, frustrate efficient and uniform breach notification to consumers.

SPECIFIC COMMENTS

ETA opposes this bill for the reasons raised above, but we have some recommendations that could help the bill better provide appropriate notification standards.

Third Party Notification

The current version of this bill is missing a third-party notification requirement would help make this bill more uniform with other state requirements and conform more seamlessly with credit card network rules.

Recommended Language

Under the Chapter 22-40 definitions section 1, please make the following changes underlined and in italics:

(6) "Third party" is an information holder that retains computerized personal or protected information in connection with providing services to another information holder.

~~(6)~~ (7) "Unauthorized person," any person not authorized to acquire or disclose personal information, or any person authorized by the information holder to access personal information who has acquired or disclosed the personal information outside the guidelines for access of disclosure established by the information holder.

Under the Chapter 22-40 section 2, please make the following changes underlined and in italics:

Following the discovery by or notification to an information holder of a breach of system security an information holder shall disclose in accordance with section 4 of this Act the breach of system security to any resident of this state whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person. *Following the discovery by or notification to a third party of a breach of system security involving computerized personal or protected information that such third party retains as a result of providing services to another information holder, the third party shall disclose in accordance with section 4 of this Act the breach of system security to such information holder, and such information holder shall be responsible for providing the required notification to affected residents.* A disclosure under this section shall be made not later than sixty days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement as provided under section 3 of this Act. An information holder is not required to make a disclosure under this section if, following an appropriate investigation and notice to the attorney general, the information holder reasonably determines that the breach will not likely result in harm to the affected person. The information holder shall document the determination under this section in writing and maintain the documentation for not less than three years.


Private Right of Action

While this bill does not, as currently drafted, provide for a private right of action, ETA opposes creating a new private right of action for data breaches. ETA looks forward to working with the Committee and the Attorney General's office to craft a solution that all sides could support, however that is unlikely if a private right of action were to be included in any new versions of this bill.

* * *

ETA thanks you for the opportunity to submit comments on this important issue. If you have any additional comments, please contact me or ETA Senior Vice President of Government Affairs, Scott Talbott at Stalbott@electran.org.

Respectfully submitted,



PJ Hoffman
Director of Regulatory Affairs
Electronic Transactions Association
PJHoffman@electran.org
(202) 677-7417

Cc: Members of House Judiciary Committee