

May 1, 2018

Chairman Darwin Booher
201 Townsend Street
Suite #3200
Lansing, MI 48933

Re: Senate Bill No. 633 (Michigan Data Breach and Data Protection)

Dear Chairman Booher:

The Electronic Transactions Association (“ETA”) opposes the SB 633 because it represents an additional hurdle in building a national uniform data breach notification framework. If enacted, SB 633 would hamper the ability of businesses to provide timely information while unnecessarily hampering critical business operations. 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 is not the best vehicle in which to address data security and data breach notification and ETA opposes SB 633.

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.

COMMENTS ON DATA SECURITY IN THE FINANCIAL INDUSTRY

ETA Supports a Tailored National Standard for Data Security. ETA believes that a tailored national framework is the most effective approach for addressing cybersecurity risks. In the electronic transactions industry, financial information data is governed by federal law, including the Gramm-Leach-Bliley Act (“GLBA”), the Federal Trade Commission’s Safeguards Rule, and robust self-regulatory programs, including the Payment Card Industry Data Security Standard (“PCI-DSS”), which sets forth requirements designed to ensure companies that process, store, or transmit credit card information maintain a secure environment for such data.

Since taking effect in 2003, for example, the information security requirements imposed by the Safeguards Rule have been held up as a model set of elements for developing an information security program. These elements have served as a foundation upon which financial institutions and services companies have built leading cybersecurity programs, leveraging the inherent flexibility of the Safeguards Rule to tailor information security practices and protocols that meet their unique business models, data use practices,

and network environments. More recently, in February 2013, President Obama released Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” which directed NIST to work with stakeholders to “develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure.” The NIST Cybersecurity Framework, released in February 2014, has seen widespread industry participation, including in the financial industry.

A Patchwork of State Laws Undermines the Effectiveness of Data Security Programs. ETA is concerned that the bill will undermine the current, effective federal and self-regulatory framework by encouraging other states to adopt similar, but potentially different data protection requirements, resulting in a patchwork of federal and state requirements for data security. This approach will force businesses to spend considerable resources interpreting and building compliance frameworks for competing regimes, while also encouraging a “check the box” approach to compliance in place of flexible, agile, and innovative programs.

The development of separate state regimes will not only increase the compliance burden of regulated entities, but also will undermine Federal efforts to develop additional national best practices and standards for cybersecurity. On October 19, 2016, for example, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency issued an advanced notice of proposed rulemaking on Enhanced Cyber Risk Management Standards. The standards would potentially apply to third party service providers. The standards would be tiered, with an additional set of higher standards for systems that provide key functionality to the financial sector. For these sector-critical systems, the agencies are considering requiring firms to substantially mitigate the risk of a disruption or failure due to a cybersecurity event.

If states continue to develop their own data security regimes, the focus of cybersecurity in the private sector will shift from developing new and innovative best practices to managing and complying with overlapping, or worse, conflicting, state and federal requirements.

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 50 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 also have the following specific concerns regarding individual sections of the bill.

Data Security Provisions

Proposed MCL 445.71 (1)(e)-(f):

This provision would require persons collecting sensitive personal information in the regular course of business and stores that information in a computerized database, to implement controls that may include

encrypting that data. However, if the person stores sensitive personal information on behalf of another person, they must do so in an encrypted form.

ETA Comments

It is unclear whether there is a practical difference between storing sensitive personal information on behalf of someone else and storing it in the regular course of business. Companies should not have to encrypt all information. This proposal is a rigid blanket technology standard which would require companies that store data on behalf of others to encrypt all data regardless of the risk levels including data which is at rest. This is much more demanding than any other state's requirements and would be beyond current industry best practices. Decisions on whether to encrypt data should be made based on a company's individual risk assessment and allow for a more nuanced, risk-based approach that aligns the level of encryption with the criticality of the data store. Additionally, companies should be able to protect data through methods other than encryption that may better facilitate innovation and offering products and services to customers.

Data Breach Provisions

Proposed MCL 445.72 (1):

This provision would maintain the current exemption for notification of breaches that "are not likely to cause substantial loss or injury" to individuals but does not provide that same exemption from notifying financial institutions.

Proposed MCL 445.72 (4):

This provision would require persons to give notice of a security breach to a financial institution that issued a credit card or debit card compromised by the breach within 3 days after the date the person discovers the security breach.

ETA Comments

Notice within three business days after discovery of a breach would move the focus from investigating and remediating a breach to reporting an alleged breach when a company may not have the full set of facts. Mandating notification within three days would create a situation in which a company could rush to report an alleged event. In fact, companies may err on the side of over-reporting events unnecessarily. Most state data breach laws allow for flexibility in reporting to permit companies to conduct a full investigation. Many states allow for notification after 30 to 45 days. When coupled with the requirement to notify financial institutions even when a breach is not likely to cause substantial loss or injury, the requirement will become extremely burdensome without the benefit of helping consumers.

Proposed MCL 445.72 (6)(c)-(e):

The provision would require the notification to include additional details including the estimated date or date range of the breach, the date of the notice, and whether notification was delayed as a result of an investigation by law enforcement.

ETA Comments

Given the requirement to notify a financial institution even when it is not likely to cause substantial loss or injury within 3 days, this level of detail makes reporting those breaches even more onerous.

Proposed MCL 445.72 (6)(k):

The provision would require a breached entity to offer “appropriate identity theft protection and mitigation services” at no cost to the affected individual for at least 12 months.

ETA Comments

ETA believes that companies should not be required to provide credit monitoring in all situations where notice is given. Given the exceptionally broad definition of sensitive personal information and notice requirements, there may be situations requiring notice where there would be no possible impact on a customer’s credit history or rating. Additionally, the bill does not describe what would be considered “appropriate identity theft prevention and mitigation services.”

Proposed MCL 445.72 (16):

This provision would allow a financial institution to bring civil suit against another entity that has a breach that contains PII for actual damages.

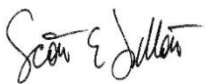
ETA Comments

ETA opposes creating a new private right of action in this instance. Creating a specific right of action for a lawsuit for issuing new credit/debit cards as a result of a breach is overreaching as these relationships are typically governed by contract. By creating a new private right of action, companies would be restricted in how they negotiate contractual responsibilities. Additionally, beyond payments, certain online lending companies currently utilize bank partners, and this provision would discourage those key partnerships by increasing liability on non-bank partners.

* * *

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

Respectfully submitted,



Scott Talbott
Senior Vice President of Government Affairs
Electronic Transactions Association