ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

March 12, 2019

Chairman Dereck Davis
House Economic Matters Committee
House Office Bldg #231
Annapolis, MD 21401

Re: House Bill No. 1127 (Data Breach, Data Protection, Money Transmission)

Dear Chairman Davis:

The Electronic Transactions Association ("ETA") opposes HB 1127 because if enacted, some parts of the bill would harm small businesses and unnecessarily hampering critical business operations without providing meaningful consumer protection. 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 HB 1127.

ETA is the leading trade association for the payments industry, representing more than 500 companies worldwide involved in electronic transaction processing products and services. 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. The NIST

Cybersecurity Framework 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.

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 Breach Provisions

Proposed 14-2504 (b)(2):

This provision would change the trigger for consumer notification of a data breach from:

- CURRENT LAW: If, after the investigation is concluded, an incident was likely that the personal information has been or will be misused.
- NEW LANGUAGE: Unless it has been reasonably determined it does not create a likelihood of a breach.

ETA Comments

The removal of the "likelihood of misuse" standard would create a hair trigger for notification and require businesses to report instances to consumers even when businesses do not have decisive reason to believe there has been or could be misuse of data. This would cause confusion and notification fatigue for consumers.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Proposed 14-2504(b)(3):
This provision would change the timeline for notification of data breaches for consumers from:

- CURRENT LAW: 45 days after the business concludes an investigation.
- NEW LANGUAGE: 10 days from discovery or notification of breach of security.

ETA Comments
Notice within 10 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 10 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 proposed change to trigger of notification, the requirement will become extremely burdensome without the benefit of helping consumers.

Proposed 14-2504(c)(2):
This provision would change the timeline for notification of data breaches for to those holding others data from:

- CURRENT LAW: As soon as practical but not later than 45 days after discovery or notification of the breach.
- NEW LANGUAGE: As soon as practical but no more than 3 days after discovery or notification of the 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 proposed change to trigger of notification, the requirement will become extremely burdensome without the benefit of helping consumers.

Proposed 14-2504(d)(2):
This provision would change the law enforcement and determining scope of breach and integrity exemption requirements from:

- CURRENT LAW: not later than 30 days after a law enforcement agency determines that it will not impede a criminal investigation but as soon as reasonably practical
- NEW LANGUAGE: not later than 1 day after a law enforcement agency determines that it will not impede a criminal investigation but as soon as reasonably practical

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

ETA Comments
Moving the timeframe from 30 days to 1 day is an extreme change and one that may not allow businesses enough time to appropriately provide notification to individuals after they receive the go-ahead from law enforcement.

Proposed 14-2504(e):
This provision changes the substitute notification format and removes the choice to send a substitute notice to consumers if the costs is more than $100,000 or that company does not have sufficient contact information. Instead companies must send substitution notification in addition to the traditional means.

ETA Comments
This proposed change allows less flexibility and not more for companies attempting to provide cost effective notices to consumers.

Proposed 14-2504(h):
The provision would add a number of specific requirements to the notification of the Attorney General after a data breach including:

- # of individuals affected
- Description of the breach including how it occurred and any vulnerabilities that were exploited
- Sample of form sent to consumers

ETA Comments
Given the extremely short timeframe for notification after a breach provided by this bill and the quick turnaround after law enforcement go-ahead, it is unlikely that a business could provide all of the required information to the Attorney General's office prior to providing notification to consumers as required by Maryland law. ETA is committed to working with law enforcement, however these new requirements, in addition to the 1-day turnaround, make it harder (in not impossible) for many businesses to comply.

Proposed 14-3504.1
This provision would allow for a new private right of action for financial institutions to file suit for the costs incurred to mitigate current or future damages resulting from a breach by a company required to institute a data security program, if there was not an adequate data security program in place and they were the proximate cause of the breach. For vendors of Financial Institutions, the same applies if their negligence was the cause of the breach.

The costs that can be recovered include:

- Notification costs
- Canceling and reissuing of cards
- Closing and re-opening accounts

There is a safe harbor from liability if:

- the data was encrypted at the time of the breach,
- the entity was PCI compliance or implemented PCI data standards, or
- compliance was determined by annual assessment within one year.

This new liability cannot be limited by other law or contract.

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 small business lending companies currently utilize bank partners to help small businesses gain access to capital, and this provision would discourage those key partnerships by increasing liability on non-bank partners.

Data Security Provisions
Proposed 14-3504.1:
This provision would require a data security program for entities that process more than $20,000 payment card transactions a year or that directly processes or transmits account information for or on behalf of another person as part of a payment processing service. That data security program may be fitted to size and nature of business. These entities could not retain account information for more than 48 hours.

ETA Comments
A tailored national framework is the most effective approach for addressing cybersecurity risks. 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.

Money Transmission Provisions
Proposed 12-414.3:
This provision prohibits money transmission licensees from engaging in a number of types of practices including:

- An unsafe or unsound act or practice;
- An unfair or deceptive act of practice;
- Fraud or intention misrepresentation;
- *Another dishonest act; or*

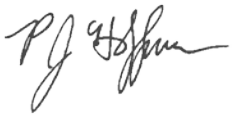
- Misappropriation of currency, virtual currency, or other value held by a fiduciary.

ETA Comments
It is unclear what would constitute "another dishonest act" without further explanation or definition.

* * *

Thank you for the opportunity to comment on this important issue. If you have any additional questions, you can contact me.

Sincerely,



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

Cc: Members of the House Economic Matters Committee
Delegate Ned Carey