STATE PRIVACY AND SECURITY COALITION

February 19, 2020

Representative Mark. K. Keller
Chair, House Commerce Committee
105 Ryan Office Building
Harrisburg, PA 17120

Representative John T. Galloway
Democratic Chair
House Commerce Committee
301 Irvis Office Building
Harrisburg, PA 17120

Re: HB 1010 (Oppose)

Dear Chairs Keller and Galloway, and Members of the House Commerce Committee,

On behalf of the State Privacy and Security Coalition, which is comprised of 30 major technology, media, communications, payment card, online security, and retail companies, and eight trade associations, we write in opposition to HB 1010. We believe Pennsylvania's current data breach statute provides effective protections for the commonwealth's residents, and do not support a private right of action for this legislation.

The primary principle of data breach notification laws is that they provide the affected residents with clear, accurate, and comprehensive information. During a data breach scenario, the breached entity is working around the clock to coordinate its various departments to determine what happened, why it happened, remediate the vulnerability, and mitigate future vulnerabilities. These departments are very likely to include Information Technology, Legal, External Affairs, and in many cases Human Resources. This is to say nothing of managing the external vendors involved in conducting the forensic investigation and any outside counsel providing legal advice, and any vendors who may also have been breached. In short, it is critically important that the breached entity have enough time to understand what occurred and clearly communicate that to affected individuals.

Accordingly, in this area of law, uniformity is beneficial to consumers. The greater the uniformity, the more efficiently notices can be provided to the affected individuals, regardless of state lines.

Pennsylvania currently has a very mainstream statute that is among the easier regimes with which to comply and understand, and is well aligned with most other states. Some states are in the process of updating their data breach elements to include more modern types of data, and we would be happy to work with the committee and the sponsor on doing so. However, HB 1010 would make Pennsylvania an outlier in its access device requirements, its strict liability provisions for breached entities, and its enforcement mechanisms.

Access Device Requirements

The bill prohibits the retention of access device information more than 48 hours after the transaction occurs.

This is an unusual provision not found in any other state breach notification law, and would cause high levels of consumer frustration. As consumers, we should have the opportunity to store our payment card information for transactions that we frequently initiate. Having to reenter credit card information for each transaction would increase the friction in a consumer transaction, with that frustration being directed at the merchant.

Additionally, payment card information is already subject to strict information security protocols through the Payment Card Information – Data Security Standards (PCI-DSS) framework.[1] Each entity at every step of the transaction process – from the issuer, to the vendor, to the acquirer/processor is required to abide by particular standards. In the same way that this bill would exempt entities who have primary regulators, this provision is unnecessary because widely adopted industry standards exist in this space.

Finally, these provisions do not reflect the current landscape of data breach security, in that payment card information is among the easiest information to change in the event of a breach. Many consumers use payment card mobile applications that alert them to possible fraudulent activity, and allow the user to put a hold or cancel a card instantly. This is not an area of consumer data that needs additional regulation.

Strict Liability for Breached Entities

The language in this bill allows financial institutions to initiate lawsuits against payment card companies following a data breach, *regardless of what the facts of the breach were*. This is a provision that has been proposed in almost every state for over 10 years, and has been rejected in every single state. This is because the provision does not consider, as examples, whether banks are themselves negligent, and whether they subscribe to card fraud screening services offered by the card brands that efficiently prevents fraud. This provision should not be considered, and we oppose this measure.

Private Right of Action

The vast majority of states – including Pennsylvania currently – do not have a private right of action for a data breach.

There are good reasons to reject private enforcement. According to a study prepared by Hogan Lovells for the U.S. Chamber Institute for Legal Reform, plaintiffs rarely recover from lawsuits brought in privacy-related cases. Instead, this litigation "often leads to a major payday for plaintiffs' attorneys, even where class members experienced no concrete harm . . . even where

[1] Available at: https://www.pcisecuritystandards.org/pci_security/standards_overview

class members may have suffered a concrete injury, the data indicates that they are unlikely to receive material compensatory or injunctive relief through private litigation."[2]

Private rights of action also open the door to class action lawsuits, which impose significant costs and do not result in meaningful benefits for consumers. One study[3] has shown that in over 150 federal class action lawsuits litigated in federal court: a) *not a single case* ended in a final judgment on the merits for the plaintiffs; b) 31% were dismissed by the courts on the merits; c) only 33% of the cases settled. When cases do settle, another study found that "the aggregate amount that class members typically receive comprises a small fraction of the nominal or stated settlement amount. Since courts base attorneys' fees on [this amount]…attorneys' fees often equate to 300%-400% of the actual aggregate class recovery."[4]

For the foregoing reasons, we oppose this HB 1010. We would be happy to discuss this matter with you further.

Respectfully submitted,

Andrew A. Kingman
General Counsel
State Privacy and Security Coalition

cc: The Honorable Members of the House Commerce Committee
Rep. Jared Solomon

[2] Mark Brennan et al., Ill-Suited: Private Rights of Action and Privacy Claims, U.S. Chamber Institute for Legal Reform at 5 (July 2019), available at: https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf

[3] *Do Class Actions Benefit Class Members? An Empirical Analysis of Class Actions* (2013), available at: https://www.mayerbrown.com/files/uploads/Documents/PDFs/2013/December/DoClassActionsBenefitClassMembers.pdf

[4] High Cost, Little Compensation, No harm to Deter: New Evidence on Class Actions Under Federal Consumer Protection Statutes, Columbia Business Law Review (2017).

STATE PRIVACY AND SECURITY COALITION

SPSC Membership List

Adobe
Amazon
Apple
Association of National Advertisers
AT&T
Business Roundtable
CapitalOne
California Cable and Telecommunications Association
CenturyLink
Charter
Comcast
CompTIA
Cox
Dropbox
Electronic Software Association
Facebook
GM
Google
H&R Block
Magazine Publishers of America
Mastercard
McKesson
Microsoft
NetChoice
Netflix
Nike
Norton Lifelock
Pinterest
Qualcomm
RELX, Inc.
SoftBank
T-Mobile
Target
TechNet
Verizon
Visa
Walgreens
Walmart

STATE PRIVACY AND SECURITY COALITION