CompTIA. The IT Industry Trade Association

February 19, 2020

Chairman Mark Keller
Democratic Chair Galloway
Pennsylvania Committee on Commerce
Nittany Lionn Inn Ballroom
200 W. Park Ave
State College, PA

RE: House Bill 1010 – Data Breach Notification of Personal Information

Dear Chairman Keller, Democratic Chair Galloway and Committee members:

On behalf of CompTIA and the technology companies we represent, I write to strongly oppose House Bill 1010. CompTIA is a non-profit trade association serving as the leading voice of the information technology industry – the driving force behind productivity growth and job creation, representing premier technology companies of all sizes. With approximately 200 member companies, 3,000 academic and training partners and more than two million IT certifications issued, CompTIA is dedicated to advancing industry growth through educational programs, market research, professional certifications and public policy advocacy.

Our members take their obligations to protect their customers' personal information very seriously. Data is of paramount importance to the information technology economy and protecting consumers' personal information is not only a responsibility of the industry, but also a crucial business practice. However, this bill would cause Pennsylvania to needlessly alter their existing statute to differ from nearly every other state in the country while providing no additional protections to consumers. We respectfully ask the Committee to reject HB 1010.

Private Right of Action

Chief among our concerns with this bill is that it will establish a private right of action for damages of up to $5,000 per violation. This is in addition to enforcement by the Attorney General. The Attorney General should have exclusive authority to enforce the act. As the elected enforcement entity in the state by the people of Pennsylvania, the AG is fully capable of ensuring the constituency is protected and laws are enforced. Allowing for a private right of action would serve to only increase litigation without meaningful preservation of consumer protections and rights. In combination with the disposal rule and reimbursement provisions outlined below, private right of action serves to punish companies that act in good faith and are working to protect consumer information as a core business function, and such provisions would send the wrong message to businesses that seek to invest in Pennsylvania.

CompTIA The IT Industry Trade Association

Disposal Rule

The bill prohibits the retention of certain financial information more than 48 hours after the transaction occurs. This requirement would add impractical burdens and challenges to businesses while not providing Pennsylvania consumers with any meaningful protections. While the goal of the provision may be to limit the potential for financial data to become subject to a breach incident, it instead would cause high levels of consumer frustration. Consumers should have the opportunity to store payment card information for ongoing relationships or frequent transactions they initiate with companies. Having to reenter credit card information for each transaction would discourage a seamless customer experience and would further direct frustration at the merchant forced to comply.

Reimbursing financial institutions

Entities that experience a breach are required to reimburse financial institutions that issue credit cards for costs related to actions taken as a result of the breach (e.g., closing/re-opening accounts, re-issuing credit cards). Financial institutions may also recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that violate the act.

A requirement to reimburse financial institutions in the event of the breach serves only to push the onus of financial losses on companies without looking at the entire incident, where the actual breach occurred and without proper risk assessment analysis. This requirement would lead to a misappropriation of resources that would be better allocated towards thoroughly investigating a suspected or confirmed breach and fixing the breach to prevent further harm. Investigations can take several weeks to determine if a breach did in fact occur, and if so, to what extent. Requiring such financial allocations would only undermine, rather than advance, the bill's goal of providing quick and accurate information about a breach and its impact on Pennsylvania residents.

The proposed changes under HB 1010 would make Pennsylvania an outlier in its reimbursement provisions and its enforcement mechanisms while simultaneously increasing consumer frustration interacting with businesses whose practices are already crucially focused on information protection. For these reasons, we respectfully urge against further consideration of this legislation as drafted. Should you have any questions, please do not hesitate to reach out to me at ddean@comptia.org or at 202.503.3641.

Sincerely,

Danielle Dean
Director, State Government Affairs
CompTIA