PA Chamber™
of Business and Industry

Feb. 21, 2020

The Honorable Mark Keller
Chair, House Commerce Committee
105 Ryan Office Bldg.
PO Box 202086
Harrisburg, PA 17120-2086

The Honorable John Galloway
Minority Chair, House Commerce Committee
301 Irvis Office Bldg.
PO Box 202140
Harrisburg, PA 17120-2140

Re: PA House Commerce Committee hearing on H.B. 1010

Dear Chairmen Keller and Galloway:

I write on behalf of the PA Chamber of Business and Industry to offer some thoughts on H.B. 1010 and issues surrounding breaches of personal data, which the Commerce Committee is scheduled to consider at a hearing on Feb. 25.

The PA Chamber recognizes the significant threat that personal data breaches pose to companies and their customers. We host regular employer conferences and roundtable events focused on IT security where industry experts both emphasize the importance of protecting data and offer guidance and best practices. We appreciate the Commerce Committee's attention to data security and encourage lawmakers to consider how best to assist employers tasked with developing internal policies and maintaining cyber security defenses against an ever-evolving and increasingly sophisticated threat.

The PA Chamber's member-driven Technology Policy position statement calls for "Balanced and reasonable cyber security measures that protect consumers and industry without imposing on Pennsylvania's businesses onerous mandates or costs." The statement also suggests that "state policymakers should further refrain from adopting public policy more burdensome or stringent than Federal policy, which could hurt Pennsylvania's competitiveness." Accordingly, while we appreciate the intent behind H.B. 1010, we are concerned with potential unintended consequences related to a number of its provisions.

Most notably, the bill establishes a private right of action and appears to all but guarantee a minimum financial recovery for every Pennsylvanian whose data is breached, even if the individual experiences no financial impact. Employers can argue they took "reasonable measures" to secure their system but that standard is subjective, unpredictable and fluid. The reality is employers, already likely incurring substantial costs to address the data security incident, and facing an imminent class action lawsuit with potentially catastrophic damages, will be pressured to simply settle the case, thereby encouraging more lawsuits against employers striving to do right by their customers.

There are questions with a number of sections, including those related to the notification timeframe, option for a substitute notice and requirements when a third-party data storage vendor is involved. Additionally, the bill omits provisions that other states have included in similar bills, including safe harbor protections for employers, risk of harm triggers for notification and exemptions for employers in industries already covered by data security laws, such as banking and healthcare. We urge you to address unanswered questions and consider adding measures to mitigate the negative unintended impacts on employers, should the Committee decide to advance legislation related to personal data security breaches.

Our most fundamental hesitation with this bill is based on our preference for a federal approach, which would avoid a patchwork of state and local laws that will be difficult for employers and consumers to navigate and could put Pennsylvania at a competitive disadvantage. That said, we understand advocates' reluctance to rely on and assume federal action and would certainly be open to further discussing this or similar legislation.

Thank you for the opportunity to provide comment on H.B. 1010 and for your attention to this important matter.

Sincerely,

Alex Halper
Director, Government Affairs

cc: The Honorable Members of the House Commerce Committee