STATE PRIVACY & SECURITY COALITION

June 7, 2022

The Honorable Kristin Phillips-Hill
Chair, Senate Communications and Technology Committee
Pennsylvania State Capitol
501 North 3rd Street
Harrisburg, PA 17120

The Honorable John Kane
Minority Chair, Senate Communications and Technology Committee
Pennsylvania State Capitol
501 North 3rd Street
Harrisburg, PA 17120

The Honorable Seth Grove
Chair, House State Government Committee
Pennsylvania State Capitol
501 North 3rd Street
Harrisburg, PA 17120

Re: **SB 696 Amendments**

Dear Chairs,

The State Privacy and Security Coalition, a coalition of over 30 telecom, retail, technology, health care, automobile, payment card companies and trade associations, appreciates the opportunity to comment on this draft with some minor but important clarifications that will help create uniformity between Pennsylvania and other states' data breach notification laws.

We recognize that the bill is a well-intentioned update to the existing state breach statute, although it includes a few provisions that would frustrate compliance and SB 696's likely intent. Specifically, we believe it is important to permit private entities—not just state agencies—to provide electronic notice in event of a breach. Furthermore, because best practices for encryption are likely to evolve with time and only represent part of an entity's larger cybersecurity program, it would be helpful to build in greater flexibility and avoid creating encryption requirements specific to Pennsylvania, which could lag technological advancements and ultimately make consumers' data less safe.

Including private entities in the electronic notice provision

The bill currently does not make it clear that entities, in addition to state agencies, may provide electronic notice to consumers. However, the bill amends the definition of Personal Information, as it applies broadly to entities, to include "A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account." As

such, it makes sense to allow for electronic notice with respect to this type of data for both state agencies and entities; doing so will accelerate notice to Pennsylvania consumers in cases where an entity discerns suspicious account activity without going through the more formal notification process.

Furthermore, existing law specifies that entities have notification obligations where notice is already defined to include "E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual." Our suggested amendment would add to this and provide entities with the same flexibility the bill creates for state agencies to use "electronic or other" forms of notice.

Anticipating evolving best practices for encryption and cybersecurity

Because best practices for encryption are constantly evolving, we also encourage greater flexibility with respect to these practices. We do not believe Pennsylvania should impose encryption standards specific to the state, as this would render it difficult if not impossible for national and global companies—with national and global encryption policies—to comply. We would question whether the executive branch is well-positioned to promulgate encryption standards across the state, as entities themselves likely are able to adopt new technologies faster and have a more nuanced understanding of the vulnerabilities they face and the tools best tailored to protect this data. Rigid standards are all the more problematic if delegated to an agency to "develop and maintain," which would also create a moving target for compliance.

Finally, encryption is only one component of an effective cybersecurity plan. We believe companies should have the flexibility to assess a variety of measures (e.g., MFA, strong passwords, de-identification, securing endpoints, etc.) to determine the best way to protect any particular set of data. Our suggested amendment refers to a more comprehensive cybersecurity program that broadens the scope of best practices while maintaining their technical feasibility in the state. This will help to future-proof the Pennsylvania law to promote cybersecurity best practices beyond encryption that have yet to be developed and deployed.

Additional Edits

Our amendments include several additional edits that add specificity and avoid unintended consequences as entities look to implement these new provisions. These include proposed language around clarifying that "medical information" is indeed just that; ensuring the entities are included when necessary; and clarifying the charge of the executive branch in determining information storage best practices.

Of course, we are happy to discuss any of these points further, and again appreciate the opportunity to participate in this process.

Respectfully submitted,

Andrew A. Kingman
General Counsel
State Privacy & Security Coalition

STATE PRIVACY & SECURITY COALITION

June 7, 2022

On behalf of the State Privacy & Security Coalition, we offer the following amendments to SB 696—Printer's No. 1330:

- Page 1, line 20: Insert OF THE after "security"
- Page 2, line 14: Insert HEALTH after "identifiable"
- Page 6, line 7: Insert THE ENTITY, after "online account," and
- Page 6, line 15: Insert THE ENTITY, after "online account with"
    - The provision regarding electronic notice needs to be expanded to include entities. Specifically, the bill currently amends the definition for PI (as it applies to broadly to entities) to include "(vi) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account." Accordingly, the provision that allows for electronic notice with respect to this type of data should also apply to entities, *in addition to* state agencies. Under the existing law, an "entity" already has notification obligations, and notice is already defined to include "E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual." The proposed edit would provide entities with more flexibility to utilize "electronic *or other*" forms of notice, as the bill already is doing for state agencies.
- Page 7, line 4: after "encryption," add in "or other appropriate and risk-based security measures"; AND
- Page 7, line 5: Insert a period after "Internet" and strike all of the following text; AND
- Page 7, lines 6-11: Strike all
    - The goal with these edits is to build in more flexibility with respect to cybersecurity practices. Encryption is only part of good cyber practices and companies should have the flexibility to assess a variety of measures (e.g., MFA, strong passwords, de-identification, securing endpoints, etc.) to determine the best way to protect any particular set of data. To this end, this flexibility will help to future-proof the PA law to promote cyber security best practices beyond encryption that have yet to be developed/deployed. Further, Pennsylvania should not have specific encryption standards, which would be difficult if not impossible for national and global companies to comply with.
- Page 7, lines 15-16: Strike "data which includes"
- Page 8, line 20: Insert a comma after "ENTITY'S"
- Page 8, line 20: Insert an apostrophe and "s" and a comma after "STATE AGENCY" so that it reads STATE AGENCY'S,