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,

PRIOR PRINTER'S NOS. 775, 793 PRINTER'S NO. 1330

THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 696 Session of 2021

INTRODUCED BY LAUGHLIN, BARTOLOTTA, STEFANO, J. WARD, HAYWOOD AND BROOKS, MAY 19, 2021

AS AMENDED ON THIRD CONSIDERATION, JANUARY 19, 2022

AN ACT

Amending the act of December 22, 2005 (P.L.474, No.94), entitled "An act providing for the notification of residents whose personal information data was or may have been disclosed due to a security system breach; and imposing penalties," further providing for title of act, for definitions and for notification of breach; prohibiting employees of the Commonwealth from using nonsecured Internet connections; ~~and~~ providing for Commonwealth policy and for entities subject to the Health Insurance Portability and Accountability Act of 1996; AND FURTHER PROVIDING FOR NOTICE EXEMPTION.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. The title of the act of December 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act, is amended to read:

AN ACT

Providing for security of computerized data and for the notification of residents whose personal information data was or may have been disclosed due to a [security system] breach OF THE SECURITY OF THE SYSTEM; and imposing penalties.

Section 2. The definition of "personal information" in

section 2 of the act is amended and the section is amended by adding definitions to read:

Section 2. Definitions.

The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

* * *

"Health insurance information." An individual's health insurance policy number or subscriber identification number ~~or any medical information in an individual's insurance application and claims history, including any appeals records.~~ IN COMBINATION WITH ACCESS CODE OR OTHER MEDICAL INFORMATION THAT PERMITS MISUSE OF AN INDIVIDUAL'S HEALTH INSURANCE BENEFITS.

* * *

"Medical information." Any individually identifiable health information contained in ~~or derived from~~ the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional.

* * *

"Personal information."

(1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

(i) Social Security number.

(ii) Driver's license number or a State identification card number issued in lieu of a driver's license.

(iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

(iv) Medical information.

(v) Health insurance information.

(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.

(2) The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.

* * *

"State agency contractor." A person that has a contract with a State agency for goods or services and a third-party ~~contractor to the contract.~~ SUBCONTRACTOR THAT PROVIDES GOODS OR SERVICES FOR THE FULFILLMENT OF THE CONTRACT.

Section 3. Section 3 of the act is amended by adding subsections to read:

Section 3. Notification of breach.

* * *

(a.1) Notification by State agency or State agency contractor.--

(1) If a State agency ~~or State agency contractor~~ DETERMINES THAT IT is the subject of a breach ~~of security of the system,~~ AFFECTING PERSONAL INFORMATION OF THE COMMONWEALTH MAINTAINED BY THE STATE OR STATE AGENCY CONTRACTOR, the State agency ~~or State agency contractor~~ shall

provide notice of the breach ~~of security of the system~~ required under subsection (a) within seven days following ~~discovery~~ DETERMINATION of the breach OR NOTIFICATION BY A STATE AGENCY CONTRACTOR AS PROVIDED UNDER PARAGRAPH (2). Notification shall be provided CONCURRENTLY to the Office of Attorney ~~General within three business days following discovery of the breach.~~ GENERAL.

(2) A STATE AGENCY CONTRACTOR SHALL NOTIFY THE CHIEF INFORMATION SECURITY OFFICER, OR A DESIGNEE, OF THE STATE AGENCY FOR WHOM THE WORK IS PERFORMED OF A BREACH OF THE SECURITY OF THE SYSTEM WITHIN SEVEN BUSINESS DAYS FOLLOWING DETERMINATION OF THE BREACH.

~~(2)~~ (3) A State agency under the Governor's jurisdiction shall also provide notice of a breach of THE security of the system to the Governor's Office of Administration within three business days following the ~~discovery~~ DETERMINATION of the breach. Notification shall occur notwithstanding the existence of procedures and policies under section 7.

~~(3)~~ (4) A State agency that, on the effective date of this section, has an existing contract with a State agency contractor shall use reasonable efforts to amend the contract to include provisions relating to the State agency contractor's compliance with this act UNLESS THE EXISTING CONTRACT ALREADY CONTAINS BREACH OF THE SECURITY OF THE SYSTEM NOTIFICATION REQUIREMENTS.

~~(4)~~ (5) A State agency that, after the effective date of this section, enters into a contract with a State agency contractor shall ensure that the contract includes provisions

relating to the State agency contractor's compliance with this act.

~~(a.2) Notification by county, school district or municipality. If a county, school district or municipality is the subject of a breach of security of the system, the county, school district or municipality shall provide notice of the breach of security of the system required under subsection (a) within seven days following discovery of the breach. Notification shall be provided to the district attorney in the county in which the breach occurred within three business days following discovery of the breach. Notification shall occur notwithstanding the existence of procedures and policies under section 7.~~

~~(a.3) Electronic notification. In the case of a breach of the security of the system involving personal information defined in section 2 for 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, the entity or State agency contractor may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the entity or State agency contractor and all other online accounts for which the person whose personal information has been breached uses the same user name or e-mail address and password or security question or answer.~~

(A.2) NOTIFICATION BY COUNTY, SCHOOL DISTRICT OR MUNICIPALITY.--IF A COUNTY, SCHOOL DISTRICT OR MUNICIPALITY IS THE SUBJECT OF A BREACH OF THE SECURITY OF THE SYSTEM, THE COUNTY, SCHOOL DISTRICT OR MUNICIPALITY SHALL PROVIDE NOTICE OF THE BREACH OF THE SECURITY OF THE SYSTEM REQUIRED UNDER SUBSECTION (A) WITHIN SEVEN DAYS FOLLOWING DETERMINATION OF THE BREACH. NOTIFICATION SHALL BE PROVIDED TO THE DISTRICT ATTORNEY IN THE COUNTY WHERE THE BREACH OCCURRED WITHIN THREE BUSINESS DAYS FOLLOWING DETERMINATION OF THE BREACH. NOTIFICATION SHALL OCCUR NOTWITHSTANDING THE EXISTENCE OF PROCEDURES AND POLICIES UNDER SECTION 7.

(A.3) ELECTRONIC NOTIFICATION.--IN THE CASE OF A BREACH OF THE SECURITY OF THE SYSTEM INVOLVING PERSONAL INFORMATION FOR 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, THE ENTITY, THE STATE AGENCY, COUNTY, SCHOOL DISTRICT OR MUNICIPALITY, TO THE EXTENT THAT IT HAS SUFFICIENT CONTACT INFORMATION FOR THE PERSON, MAY COMPLY WITH THIS SECTION BY PROVIDING THE BREACH OF THE SECURITY OF THE SYSTEM NOTIFICATION IN ELECTRONIC OR OTHER FORM THAT DIRECTS THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN BREACHED TO PROMPTLY CHANGE THE PERSON'S PASSWORD AND SECURITY QUESTION OR ANSWER, AS APPLICABLE OR TO TAKE OTHER STEPS APPROPRIATE TO PROTECT THE ONLINE ACCOUNT WITH THE ENTITY, THE STATE AGENCY, COUNTY, SCHOOL DISTRICT OR MUNICIPALITY AND OTHER ONLINE ACCOUNTS FOR WHICH THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN BREACHED USES THE SAME USER NAME OR E-MAIL ADDRESS AND PASSWORD OR SECURITY QUESTION OR ANSWER.

(A.4) AFFECTED INDIVIDUALS.--IN THE CASE OF A BREACH OF THE SECURITY OF THE SYSTEM INVOLVING PERSONAL INFORMATION FOR 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, THE STATE AGENCY CONTRACTOR MAY COMPLY WITH THIS SECTION BY PROVIDING A LIST OF AFFECTED RESIDENTS OF THIS COMMONWEALTH, IF KNOWN, TO THE STATE AGENCY SUBJECT OF THE BREACH OF THE SECURITY OF THE SYSTEM.

* * *

Section 4. The act is amended by adding sections to read:

Section 5.1. Encryption required.

(a) General rule.--State employees and State agency contractor employees shall, while working with personal information on behalf of the Commonwealth or otherwise conducting official business on behalf of the Commonwealth, utilize encryption or other appropriate and risk-based security measures to protect the transmission of personal information over the Internet ~~from being viewed or modified by a AN UNAUTHORIZED third party~~.

~~(b) Transmission policy. The Governor's Office of Administration shall develop and maintain a policy to govern the proper encryption and transmission by State agencies under the Governor's jurisdiction of data which includes personal information.~~

Section 5.2. Commonwealth policy.

(a) Storage policy.--The Governor's Office of Administration shall develop a policy to govern the proper storage by State agencies under the Governor's jurisdiction of ~~data which~~

~~includes~~ personal information. The policy shall address identifying, collecting, maintaining, displaying and transferring ~~personally identifiable~~ PERSONAL information, using ~~personally identifiable~~ PERSONAL information in test environments, remediating ~~personally identifiable~~ PERSONAL information stored on legacy systems and other relevant issues. A goal of the policy shall be to reduce the risk of future breaches of THE security of the system.

(b) Considerations.--In developing the policy, the Governor's Office of Administration shall consider similar existing FEDERAL AND OTHER policies in other states, best practices identified by other states and relevant studies and other sources as appropriate.

(c) Review and update.--The policy shall be reviewed at least annually and updated as necessary.

Section 5.3. Entities subject to the Health Insurance Portability and Accountability Act of 1996.

Any covered entity or business associate that is subject to and in compliance with the privacy and security standards for the protection of electronic PERSONAL health information established under the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, 110 Stat. 1936) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, 123 Stat. 226-279 and 467-496) shall be deemed to be in compliance with the provisions of this act.

SECTION 5. SECTION 7(B)(2) OF THE ACT IS AMENDED TO READ:

SECTION 7. NOTICE EXEMPTION.

* * *

(B) COMPLIANCE WITH FEDERAL REQUIREMENTS.--

* * *

(2) AN ENTITY, A STATE AGENCY OR STATE AGENCY CONTRACTOR THAT COMPLIES WITH THE NOTIFICATION REQUIREMENTS OR PROCEDURES PURSUANT TO THE RULES, REGULATIONS, PROCEDURES OR GUIDELINES ESTABLISHED BY THE ENTITY'S, STATE AGENCY'S, OR STATE AGENCY CONTRACTOR'S PRIMARY OR FUNCTIONAL FEDERAL REGULATOR SHALL BE IN COMPLIANCE WITH THIS ACT.

Section ~~5~~ 6. This act shall take effect in ~~60~~ 120 days.