ATTORNEY GENERAL WILLIAM TONG
STATE OF CONNECTICUT

House Bill 5310, *An Act Concerning Data Privacy Breaches*

Chairman D'Agostino, Ranking Member Rutigliano, Chairman Maroney, Ranking Member Witkos and distinguished members of the General Law Committee, thank you for the opportunity to testify before you today in strong support of HB 5310, *An Act Concerning Data Privacy Breaches*. This bill passed out of the General Law Committee during the abbreviated session last year and the language before you today is largely the same. Additionally, please note that substitute language, borne out of productive discussions with a coalition of regulated entities, is included at the end of this testimony for your consideration.

In 2005, the Connecticut General Assembly passed one of our nation's first laws protecting consumers from online data breaches, and in doing so, made our state a national leader in data privacy. Since then, as technology and our understanding of the risks associated with living in an online world have evolved, dozens of other states passed and updated their own data breach laws to keep up with that evolution. In 2019 alone, 9 states passed new and expanded data breach notification laws and in 2020, 6 states passed privacy-related legislation. This underscores the importance of updating our statute; it is time for Connecticut to catch up.

House Bill 5310 updates Connecticut's breach notification statute. It strengthens consumer protections by broadening the definition of "personal information," shortening the time period to notify consumers and the Office of the Attorney General of a security breach from 90 to 60 days, and by improving notification procedures for security breaches involving the compromise of online account credentials. Finally, it would provide confidentiality for material obtained by our office through Civil Investigative Demands.

Broadening the Definition of "Personal Information"

At the core of our breach notification statute, Section 36a-701b of the Connecticut General Statutes, is the definition of "personal information." These definitional categories, or identifiers, are what trigger breach notice requirements and therefore determine whether our Office and affected individuals are alerted when their most sensitive information may have been compromised. Without such notice, our enforcement ability is diminished and individuals may be unable to take timely steps to protect themselves from identify theft.

Connecticut's current definition of "personal information" covers some of the most sensitive personal identifiers, including Social Security numbers and financial account information. However, this definition does not capture the full spectrum of information that may be used to perpetrate identity theft.

To ensure that our data breach notification statute is effective in protecting Connecticut residents against identity theft, the definition of "personal information" must be broadened to include additional categories of sensitive information. It must also be versatile enough to respond to new types of technology capable of exposing individuals to identity theft.

With this goal in mind, Section 1(a) expands the definition of "personal information" to include the following data elements: (1) a passport number, military identification number or government issued identification numbers; (2) an individual tax identification number (ITIN) and an identity protection personal information number (IP PIN); (3) medical information, including information about an individual's mental health; (4) health insurance information; (5) biometric data; and (6) online account information.

Including these identifiers in the breach notification statute would require that our Office and Connecticut residents be notified when this information is compromised in a security breach. Notification will allow consumers to better protect themselves from identity theft, enable our Office to respond nimbly to consumers who seek our assistance, and ensure that we continue to play a leading role in any subsequent multistate investigations.

With respect to the added identifiers, it is important to once again note that we are playing catch-up with our sister states. For example, 21 states, including our neighbors New York and Rhode Island, already include "medical information" within their statutes' definition of personal information. State Attorneys General have the authority to enforce HIPAA, the federal law that protects medical information, so it is vitally important that our Office receive notice of HIPAA breaches impacting Connecticut residents.

Similarly, with the advent of exploitation of online account credentials, it is no surprise that 18 states have already passed amendments to their breach notification statutes protecting this information. Online account information can be used to gain access to an individual's most sensitive accounts, thereby exposing additional information that may enable an attacker to perpetrate identity theft.

Finally, biometric data is also of increasing importance. The uniquely personal nature of this information presents a heightened risk to individuals and offers tremendous value to cyber criminals.

Shortening Notification Time Period

Section 1(b)(1) shortens the outside limit in which entities subject to the statute must notify individuals of security breaches from 90 days to 60 days. The reduction of the outside limit to 60 days is in line with recent amendments to a number of other states' data breach notification windows.

Connecticut residents must be informed as quickly as possible when their information is at risk so that they may take the appropriate action to protect it. A three month notification delay is no longer acceptable in today's fast paced world—where an identity theft can take place in mere hours or days after compromise.

Improved Notification Procedures

Section b(1) includes new language for your consideration regarding circumstances where it may take a company longer than 60 days to identify the full impacted population of Connecticut residents. In that scenario, this new language would require the notifying entity to notify as many impacted Connecticut residents as have been identified within those 60 days, then proceed in good faith to identify and provide notice to any additional Connecticut residents as expediently as possible. This language is designed to ensure that notification is not unreasonably delayed on the grounds that an investigation into the scope of the breach may take months to complete.

Section 2(g) addresses notification procedures for security breaches involving online account credentials. Our current statute permits entities to provide individual notification electronically, which include notification via an online account—such as an e-mail address—that may have been compromised in the security breach. This bill would require entities to use an additional method of notification when an online account may have been compromised to ensure that impacted individuals are able to receive the notification. Ten states include similar specifications in their breach notification statutes. New York was the latest to implement such a requirement through its NY SHIELD law.

Investigative Confidentiality

Finally, Section 2(i) would afford confidentiality to responses to a Civil Investigative Demand ("CID") issued in connection with data breach investigations. Such investigations inherently involve highly technical, sensitive materials related to information security. Protecting these CID responses will ensure that our office can appropriately request and review security-related materials, while ensuring that bad actors are not made aware of any vulnerabilities that they might exploit in a future breach.

For all the foregoing reasons, I ask for your support of expanding consumer data protections through HB 5310. Thank you once again for the opportunity to offer testimony and please do not hesitate to contact me with any questions or concerns.

General Assembly

Raised Bill No. 137

February Session, 2020

LCO No. **1415**

*01415_____GL_*

Referred to Committee on GENERAL LAW

Introduced by:
(GL)

AN ACT CONCERNING DATA PRIVACY BREACHES.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. Section 36a-701b of the general statutes, as amended by section 231 of public act 19-117 and section 9 of public act 19-196, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2021*):

(a) For purposes of this section, (1) "breach of security" means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable; and (2) "personal information" means (A) an individual's first name or first initial and last name in combination with any one, or more, of the following data: [(A)] (i) Social Security number; (ii) individual taxpayer identification number; ~~or~~(iii) identity protection personal identification number issued by the IRS; [(B)] (~~iii~~iv) driver's license number, [or] state identification card number, passport number, military identification

number, or other identification number issued by the government that is commonly used to verify identity; [(C)] (iv) credit or debit card number; [or (D)] (vi) financial account number in combination with any required security code, access code or password that would permit access to such financial account; (vii) medical information~~, including any information~~ regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (viii) health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer ~~or a self-insured employer~~ to identify the individual; or (~~viii~~ix) biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics ~~and~~ used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image~~, or other unique physical representation or digital representation of biometric data~~; and (B) user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

(b) (1) Any person who [conducts business in this state, and who, in the ordinary course of such person's business,] owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was breached or is reasonably believed to have been breached. Such notice shall be made without unreasonable delay but not later than [ninety] ~~thirty~~ sixty days after the discovery of such breach, unless a shorter time is required under federal law, subject to the provisions of subsection (d) of this section [~~and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system.~~] If the person identifies additional residents of this state whose personal information was breached or reasonably believed to have been

breached following sixty days after the discovery of such breach, the person shall proceed in good faith to notify such additional residents as expediently as possible. [Such notification] Notification shall not be required if, after an appropriate investigation [~~and consultation with relevant federal, state and local agencies responsible for law enforcement,~~] the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired [and] or accessed.

(2) If notice of a breach of security is required by subdivision (1) of this subsection:

(A) The person who [conducts business in this state, and who, in the ordinary course of such person's business,] owns, licenses or maintains computerized data that includes personal information, shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General; and

(B) The person who [conducts business in this state, and who, in the ordinary course of such person's business,] owns or licenses computerized data that includes personal information, shall offer to each resident whose [~~nonpublic~~] personal information under [subparagraph (B)(i) of subdivision (9) of subsection (b) of section 38a-38 or personal information as defined in] clauses (i) or (ii) of subparagraph (A) of subdivision (2) of subsection (a) of this section was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twenty-four months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file.

(c) Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the

data immediately following its discovery, if the personal information of a resident of this state was breached or is reasonably believed to have been breached.

(d) Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.

(e) Any notice to a resident, owner or licensee required by the provisions of this section may be provided by one of the following methods, subject to the provisions of subsection (~~g~~f) of this section: (1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001; (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this subsection would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or that the person does not have sufficient contact information. Substitute notice shall consist of the following: (A) Electronic mail notice when the person has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the web site of the person if the person maintains one; and (C) notification to major state-wide media, including newspapers, radio and television.

(f)(1) In the event of a breach of login credentials under subparagraph (B) of subdivision (2) of subsection (a) of this section, notice to a resident may be provided in electronic or other form that directs the resident whose personal information was breached or is reasonably believed to have been breached to promptly change any password or security questions and answer, as applicable, or to take other appropriate steps to protect the affected online account and all other online accounts for

which the resident uses the same user name or email address and password or security question and answer.

(2) Any person that furnishes an email account shall not comply with this section by providing notification to the email account that was breached or reasonably believed to have been breached. The person shall provide notice by another method described in this section or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person knows the resident customarily access the account.

(~~f~~g) Any person that maintains such person's own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies, as applicable, residents of this state, owners and licensees in accordance with such person's policies in the event of a breach of security and in the case of notice to a resident, such person also notifies the Attorney General not later than the time when notice is provided to the resident. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided (1) such person notifies, as applicable, such residents of this state, owners, and licensees required to be notified under and in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security, and (2) if notice is given to a resident of this state in accordance with subdivision (1) of this subsection regarding a breach of security, such person also notifies the Attorney General not later than the time when notice is provided to the resident.

(h) Any person that is subject to and in compliance with the privacy

and security standards under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act ("HITECH") shall be deemed to be in compliance with this statute, provided that (i) any person required to provide notification to Connecticut residents pursuant to HITECH shall also provide notice to the Attorney General not later than the time when notice is provided to such residents and (ii) the person otherwise complies with the requirements of subparagraph (B) of subdivision (2) of subsection (b) of this section.

~~(g) In the event of a breach of login credentials under subparagraph (B) of subdivision (2) of subsection (a) of this section, notice to a resident shall not be exclusively provided through the affected online account, but shall be provided via methods otherwise permitted pursuant to subsection (e) of this section.~~

(i) All documents, materials and information provided in response to an investigative demand issued pursuant to section 42-110d(c) in connection with the investigation of a breach of security as defined by this section shall be exempt from public disclosure under section 1-210(a) provided that the Attorney General may make such documents, materials or information available to third parties in furtherance of such investigation.

[(g)**]** (~~h~~j) Failure to comply with the requirements of this section shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced by the Attorney General.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2021*	36a-701b

Statement of Purpose:
To expand the data privacy breach notification statute to protect consumers.

[Proposed deletions are enclosed in brackets. Proposed additions are indicated by underline, except that when the entire text of a bill or resolution or a section of a bill or resolution is new, it is not underlined.]