STATE PRIVACY AND SECURITY COALITION

April 12, 2019

Representative Michael Marcotte
Chairman, House Commerce and
Economic Development Committee
Vermont State House Room 35
115 State Street
Montpelier, VT 05633

Representative Jean O'Sullivan
Vice Chair, House Commerce and
Economic Development Committee
Vermont State House Room 35
115 State Street
Montpelier, VT 05633

Re: Senate Bill 110 – Data Breach Notification Provisions

Dear Mr. Chairman, Madame Vice Chair, and Members of the Committee,

The State Privacy & Security Coalition, a coalition of 23 leading media, technology, retail, payment card, and online security companies, and six trade associations, writes to respectfully propose amendments and feedback to the current language added yesterday to the data breach provisions of SB 110.

This draft was released late yesterday, and contains a lot of new data elements triggering breach notice and additional language that are not found in any of the 50 state breach notice laws, and that have not been in either the drafts released prior to session, the versions discussed in the Senate, or in the versions about which I testified for two days earlier this week.

We request that the committee take more time to analyze these changes, narrow the scope to the elements and language being discussed earlier this week and continue the discussion on those points, or move this bill to a study to assess the impact and potential for unintended consequences that could flow from this new language.

There are two critical points that we ask the committee to keep in mind: First, Vermont already has the strictest data breach notification statute in the country. It requires rapid notice to the Attorney General's Office within 14 days when any of the data elements in the State's breach notice law is reasonably believed to have been acquired. As a practical matter this means hiring a lawyer and often a computer forensics firm to figure out if data may have left the company systems. It costs time and money. This is appropriate for data elements that create risk to Vermont residents, but is wasteful for data that do not create risk. Introducing some of the provisions floated in last night's draft of S.110 would make Vermont even more of an outlier than it already is without adding a meaningful benefit to consumers.

Second, specificity as to what requires notice is good public policy, both to provide clear guidance to breached entities about what (costly) computer forensics searches should look for in the wake of a suspected breach, and to establish when notice is required.

Third, conformity of notice laws across state lines for data breach notification statutes is a good thing – it helps expedite consumer notices because businesses and their compliance counsel do not have to spend extra time creating separate notices to meet differing state notice requirements – a process that is costly to businesses and can delay notice to consumers.

Social Security Number Sufficient to Trigger Notice (9)(A)

We urge the committee to remove this provision. Social Security Numbers are sensitive information, and breaches involving this data element are treated with the utmost gravity by the breached entity. However, this formulation of a data breach notification would trigger 14-day AG notice obligations and individual notice obligations ***when the breached entity does not know whose personal information has been breached***, much less that the breach relates in any way to Vermont. Put another way – a company would be subject to state enforcement if a hacker acquired only social security numbers and an email account password, ***without knowing who the consumer is.*** This is why every other state in the nation requires corroborating information – first initial and last name, or a full name.

This proposal would put Vermont businesses in a catch-22 situation: it would place them in violation of the law when they do not have any information about whom to notify.

We suggest that SSN be deleted as an alternative to name and the removal of references to social security numbers in sections (d)(3) and (d)(4).

Government ID Numbers (9)(A)(i)

We agree that driver's license military ID number plus name should require notice. However, "driver's identification number" is unclear, as is an "other similar number used to verify identity." Does this include a voter registration card or fishing or hunting license number, for example, if used on rare occasion to verify identity, even though these ID numbers cannot be used to commit identity theft or fraud?

Health Information Data Element 9(A)(vii)

As discussed throughout the week, Oregon's definition of the health information data element is very broad and unintentionally sweeps in everyday conversation and disclosures made by individuals about friends or acquaintances (for example, a social media post congratulating a friend on their pregnancy, or an email from someone about their time completing a 10k run.).

We ask that you amend the definition of health information to bring it in line with the overwhelming majority other state statutes including health information as an element of Personal Information. We propose that this element read as follows, either:

> Any information about a consumer's medical or mental health treatment or diagnosis by a health care professional.

OR

> Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health-care professional, or deoxyribonucleic acid profile (Delaware's health data definition).

Of the 17 states that include Health Information as a data element in their data breach laws, only 4 do not include language tying "health information" to treatment or diagnosis by a health care professional. The language still requires notice for information far beyond a breach of medical records, as well as individuals' communications about a health diagnosis or treatment, but it avoids requiring Vermont businesses in the wake of data breach from conducting costly eDiscovery-style searches for statements like "I have a cold today" or "I can run a mile in 9 1/2 minutes".

Particularly because Vermont requires notice to the AG's Office of *all* acquisition of breach notice data elements to the AG's Office regardless of whether there is any risk of harm, it makes sense to increase the specificity here and conform with the direction other states have taken.

HIPAA Exemption

Because Vermont is considering adding health information as a data element, it is critically important that an exemption for information subject to the federal Health Information Portability and Accessibility Act (HIPAA) be added as well. Information subject to HIPAA is already subject to federal data breach notifications.

Every state that has health information as a data element also contains a HIPAA exemption for this reason. We propose the following language:

> Any person subject to this chapter which maintains procedures for security breach notification pursuant to the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, as amended) (HIPAA) is deemed to be in compliance with this chapter if the person notifies affected Vermont residents in accordance with the maintained procedures when a breach of security occurs.

STATE PRIVACY AND SECURITY COALITION

Conclusion

Effective and clear data breach notification statutes are important pro-cybersecurity tools. The language we have offered improves both the specificity and the clarity of the statute, while avoiding non-conformity across state lines.

As always, we are happy to discuss these changes at your convenience.

Respectfully submitted,

Andrew A. Kingman
Counsel
State Privacy & Security Coalition.