STATE PRIVACY & SECURITY COALITION

January 27, 2021

Chairwoman Delores G. Kelley
Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, MD 21401

Chairman Dereck Davis
Economic Matters Committee
House Office Building, Room 231
6 Bladen St., Annapolis, MD 21401

Re: MD SB 16/218 (Oppose)

Dear Chairwoman Kelley and Chairman Davis,

On behalf of the State Privacy and Security Coalition, a coalition of 29 leading retail, technology, telecommunications, automobile, online security, and payment card companies, we write in opposition to SB 16 and HB 218, which seeks to replicate the 2008 Illinois Biometric Information Privacy Act (BIPA). Our members recognize the importance of consumer privacy and the sensitivity of biometric data that can identify individuals or authenticate their identities. At the same time, they are vigilantly, proactively working to keep their users, subscribers, and customers safe. These bills would make this more difficult and put Maryland citizens at much greater risk of fraud because biometric data is a leading means of fraud prevention.

The language in these bills is taken from BIPA - a bill that was passed in 2008 (less than a year after the invention of the smartphone). It imposes unworkable requirements and does not recognize the important uses of biometric data in fraud prevention. Importantly, no other state has passed this bill in the twelve years since its enactment. It is the basis of hundreds of frivolous lawsuits that have deterred many companies from using voice recognition and other biometric data to prevent fraud; use fingerprints as alternatives for punch-cards; and for deploy pro-consumer services in Illinois' innovation economy, such as doorbells that elderly residents can use to determine who is at their door. If this bill were to pass, it would make voice recognition fraud prevention services untenable in Maryland and burden state businesses with unnecessary compliance costs for ordinary business operations. Maryland should not follow Illinois' lead.

These bills ignore the modern online ecosystem and disadvantages the disabled population

One of the biggest problems with this law's evolution in Illinois is that it fails to recognize the fundamental differences between consumer-facing entities and those entities' vendors. In Illinois, plaintiffs' lawyers have filed scores of class action lawsuits alleging that vendors, *which never interact with consumers*, have violated the statute by not obtaining consumers' the proper consent. Because this is entirely impractical, this is predatory behavior that has no relation to the intent of the statute, pro-privacy practices, or protecting consumers. Maryland would not be well-served by adopting this regime.

Business and consumers have become accustomed to this more modern structure in nearly every privacy and cybersecurity statute in the country – from breach bills that distinguish between responsibilities of "owners" of information versus "maintainers," to privacy legislation that distinguishes between controllers (who determine the "means and purposes of the processing" of data) and processors (who process personal data on behalf and at the direction of a controller).

Without this most fundamental distinction, the bill will be unworkable and will lead to untenable litigation exposure even as entities attempt to comply in good faith.

Moreover, the bill's lack of flexibility disadvantages the disabled community. By providing only one method of providing consent – in writing – the bill deprives individuals who do not have the use of their hands the ability to avail themselves of the convenience and security advantages of products that use biometrics.

The bill has no exception for fraud prevention

Biometric data is used today for security, authentication, and fraud prevention purposes that this bill would make totally untenable. For example, biometric data is used to secure access to highly sensitive buildings, to detect fraudulent callers, and to improve security on financial accounts. It has also been used to help track the violent extremists who attacked the US Capitol on January 6th and who pose a serious threat of violence in Maryland and many other states.

Because the bill does not allow for the use of biometric data for fraud prevention without written opt-in consent – and does not even have a clear security exception – the bill would put Maryland residents at great risk of fraud and security threats. Fraudsters, terrorists and other criminals will not consent to use of their biometric data for fraud prevent and security purposes, so they would not be able to be screened by private businesses.

In Illinois, the only state with class action enforcement of the state's biometric privacy law, businesses are avoiding using biometric data for fraud or security purposes because of the huge class action risk.

This issue is even more acute in the post-COVID-19 era. Cybersecurity has never been more important, and the pandemic has resulted in an exponential increase in cybercrime activity against both private and public sector entities. It is critical for the safety to both sectors that Maryland not unintentionally remove an important tool to leverage in combatting cyber threats and preserving secure systems and identities.

The liability exposure created by the bill would create huge risk for companies and increase risk to Maryland residents.

The bill would create very large class action litigation exposure for any alleged violations of the law by commercial entities, significantly deterring uses of biometric data for fraud prevention, security and other beneficial purposes. The result would be to enrich trial lawyers without striking a balance that allows use of biometric data for purposes significantly benefitting Maryland residents and businesses. The numbers bear this out: in the last five years, trial lawyers have filed ***almost 900 class action lawsuits based on BIPA.*** **In January 2021 alone, we have already seen 44 class action lawsuits filed – in 15 business days.** Twelve years of experience with Illinois' law have shown that this approach leads

businesses to decline to offer their full suite of services to state residents or avoid offering their services in the state at all due to the overzealous litigation this legislation catalyzed.

For these reasons, our coalition opposes these bills. We believe that a study commission is the best mechanism for discussion so that these issues can be carefully examined and more clearly defined.

Respectfully submitted,

Andrew A. Kingman
General Counsel
State Privacy and Security Coalition