SB11: Maryland Online Consumer Protection and Child Safety Act
Senate Finance Committee
January 26, 2022

Position: Unfavorable

Background: SB11 regulates the collection and use of consumers' personal information by businesses; establishing the right of a consumer to receive information regarding collection practices, have personal information deleted by a business, and prohibit the disclosure of personal information by a business; requiring businesses to provide certain notices to consumers and include certain information in online privacy policies; and authorizing the Office of the Attorney General to adopt regulations to carry out the Act.

Comments: The Maryland Retailers Association has numerous concerns with the legislation as outlined below.

1. **California's Privacy Model is the Wrong Model for Maryland**: S.B. 11, exclusively regulates "businesses" (e.g., retailers and other consumer-facing Main Street businesses) while exempting service providers and third parties who also handle the majority of consumer data. In this respect, it is following a California privacy law model, but it also goes beyond it in some respects. Maryland should be looking toward a more balanced law that obligates <u>all parties</u> that handle data to protect it and honor consumers' choices with respect to it.
    a. **MD Should Consider the VA Model**: Virginia's Consumer Data Protection Act (CDPA) was broadly supported by industry. It was adopted last spring and will take effect on January 1, 2023. It was the model for the only two state privacy bills to be enacted in 2021: in Virginia and Colorado. Unlike SB11, the VA privacy law balances the particular obligations between businesses and service providers. Additionally, with VA bordering Maryland and DC, it would make much more sense in this region to have a more harmonized privacy law – the same obligations for businesses and identical rights for consumers – across the three jurisdictions in light of consumers traversing these state and district lines daily and retailers being located in three separate jurisdictions in one metropolitan region.

2. **S.B. 11 Would Outlaw Retailers' Customer Loyalty Plans Unless Robust Savings Clauses Are Adopted**: Retailers are heavily invested in customer loyalty programs. The business incentive for loyalty programs is to reward repeat customers who sign up for the program for their shopping loyalty, and to create incentives for customers to shop at a particular brand repeatedly. Forrester Research released a report a few years ago that confirmed how popular such loyalty programs are with consumers: approximately 80% of adults participate in loyalty programs, and the average adult participant is signed up

for nine programs. Despite consumers supporting and opting into these programs, the current nondiscrimination language in S.B. 11 (p. 14, l. 21 – p. 15, l. 2) would render unlawful the normal functioning of retailers' customer loyalty programs. The programs are intended to benefit the loyal customers participating in them by offering them better prices and levels of service compared to those customers who do not participate in the programs.

For example, a consumer may exercise a right to opt-out of third party disclosure under the bill, but if such third party disclosure is necessary for the tracking of the customer's activity and/or the delivery of the loyalty plan benefits under the program, then the customer would not be able to participate in the loyalty program. That customer who opted out (i.e., exercising a privacy right) could then claim a violation of the bill's nondiscrimination provision if other customers who continue to participate in the plan receive better prices or different levels of quality of good or services by being in the plan. Retailers have therefore actively opposed similar nondiscrimination provisions in other states unless and until a loyalty plan savings clause has been adopted to preserve the loyalty programs that consumers overwhelmingly desire to have. We would strongly recommend S.B. 11 be revised to add the same savings clauses, to ensure that retailers have loyalty plan protections.

a. **Language Recommendations**: Although Virginia language could be used to rectify this deficiency, we would recommend using the following language from Ohio's legislation:

> **Sec. 1355.09.** (A) Subject to divisions (B) and (C) of this section, a business shall not discriminate against a consumer for exercising the rights provided to a consumer under this chapter.
> (B) A business may charge different prices or rates for goods or services for individuals who exercise their rights under this chapter for legitimate business reasons or as otherwise permitted or required by applicable law.
> (C) A business's denial of a consumer's request in compliance with this chapter shall not be considered discrimination against the consumer.
> (D) Nothing in this section shall be construed as doing either of the following:
> (1) Requiring a business to provide a product or service that requires the personal data of a consumer that the business does not collect or maintain or requiring a business to provide a product or service if the consumer has exercised the right to opt-out pursuant to section 1355.08 of the Revised Code;
> (2) Prohibiting a business from offering a different price, rate, level, quality, or selection of goods or services

to a consumer, including offering goods or services for no fee, if the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

3. **S.B. 11 Does Not Place Any Obligations on Service Providers or Third Parties Who Handle the Most Consumer Data.** As noted in the first point above, S.B. 11 exclusively regulates "businesses" (e.g., retailers and other consumer-facing Main Street businesses) while exempting "service providers" and "third parties" who handle the majority of consumer data. As a result, all liability for violations of the bill – even violations that arguably are the fault of a service provider – will land on the businesses that contracted the service provider, even if that business itself has done everything required of it under the law.
    a. **Example of How Retailers May be Vicariously Liable for Service Providers' Privacy Failures Under the Bill.** For example, if a consumer exercises a privacy right (e.g., delete consumers' personal information upon request), it is the obligation of the business under S.B. 11 to fulfill that obligation alone, even if it requires the assistance or performance by a service provider (e.g., cloud services) in order to complete the request. In subsection 14-4406(C) (p. 12, l. 15), for instance, it states: "(C) A **BUSINESS** THAT RECEIVES A VERIFIABLE CONSUMER REQUEST FROM A CONSUMER TO DELETE THE CONSUMER'S PERSONAL INFORMATION UNDER SUBSECTION (A) OF THIS SECTION **SHALL DELETE** THE PERSONAL INFORMATION FROM ITS RECORDS **AND DIRECT SERVICE PROVIDERS** TO DELETE THE PERSONAL INFORMATION FROM THE SERVICE PROVIDERS' RECORDS." Notably, the obligation in S.B. 11's section here is on the business alone to delete the personal information (PI) -- and to "direct" service providers to delete the PI as well – but there is no obligation in S.B. 11 on the service provider to actually delete the PI (i.e., the bill does not say the service provider "shall" delete) and the service provider is not even obligated to assist the business in fulfilling the obligation to delete where it is necessary to do so (i.e., where the PI is in service providers' database or cloud, for instance, that is controlled by the service provider). This means that if the service provider fails to take action and does not delete the PI in the database or cloud, the business "directed" it to, it will be the business (not the service provider that failed) who is liable under the statute for that failure if a consumer claims harm from continued accessibility to his/her PI in the database or cloud after making the deletion request and the AG then takes action to address it. In order to place liability where it belongs – on the service provider in this example – S.B. 11 would need to have obligations, such as those in VA and CO, that require the service provider (defined as a "processor" in those laws) to assist the business in meeting its obligations. We strongly recommend that S.B. 11 be revised to adopt provisions such as those in

the newly enacted VA and CO privacy laws, modeled on language in the WA privacy bill, that creates important obligations for data processors. This language protects both consumers and businesses alike in the handling of customers' PI by establishing the necessary statutory requirements for service providers to abide by consumers' privacy rights requests. Virginia's service provider (a.k.a. processor) language would rectify this deficiency.

- **Minimum Requirements of Other Providers:** Common-sense, minimum requirements for service providers (i.e., data processors) similar to those adopted in other state privacy laws should be added. This language would ensure that S.B. 11 protects consumers' personal information where the majority of consumer data processing occurs, by requiring such data processors to honor consumers' rights requests, protect consumer data provided to it by a business, and abide by other standard processor privacy obligations (listed in bullet form below). It would also ensure that privacy obligations do not fall exclusively on Main Street businesses such as retailers when the majority of data processing occurs among their service providers. Presently, S.B. 11 fails to protect consumers comprehensively by omitting privacy obligations for service providers to protect consumers' personal information and/or to honor their privacy rights requests. The language from WPA (in the form that passed the Washington Senate by a vote of 48-1 in 2021) included the following basic data processor obligations that were enacted in two other state laws and that also have applied to many U.S.-based global data processors under the EU's GDPR since 2018 – they require service providers (i.e., defined as "processors" under the state laws and GDPR) to:
  - fulfill the business's obligation to respond to consumer privacy rights requests and provide security in processing required by the act;
  - assist the business in meeting its obligations in relation to the security of processing the personal information and in relation to the notification of a security breach;
  - ensure each person processing personal information at the service provider is subject to a duty of confidentiality with respect to the data;
  - require any subcontractor of the service provider, pursuant to a written contract, to meet the service providers' obligations to the business with respect to the data;
  - implement appropriate technical and organizational measures to ensure the service provider adopts a level of security appropriate to the risk;
  - delete or return to the business, at the business's direction, all personal information in the possession of the service provider at the end of the provision of services;

- § make available, upon the reasonable request of a business, all information necessary to demonstrate the service provider's compliance with the act; and
- § cooperate with reasonable audit assessments by the business or its designator auditor of the service provider's policies and technical and organizational measures in support of the act's obligations for businesses and service providers.

- o **Suggested revision to text of S.B. 11:** Add to S.B. 11 the processor obligations found in Section 106 of S.B. 5062, the Washington Privacy Act (WPA) *(in the form that passed the Washington Senate by a vote of 48-1 in the 2021 session)*. (Note, the text of the WPA would first need to be modified by replacing all instances of the WPA-defined term "controller" with the term "business" (as defined in S.B. 11), replacing all instances of the WPA-defined term "processor" with "service provider" (as defined in S.B. 11), and making similar technical corrections to ensure the language works with S.B. 11's definitions of "personal information.")

For these reasons as well as the aggressive Title 13 penalties even for retailers following the law and broad exceptions included in the bill, we must again urge an unfavorable report on this legislation. Thank you for your consideration.