Testimony for VT Committee
March 14, 2024 – 2:00pm EST

Thank you Chair Marcotte, Madame Vice Chair Jerome and Members of the Committee.

My name is Kellie Beckman and I am General Counsel for Appriss Retail. Appriss Retail is a Software as a Service Company that provides solutions to Retailers to assist them in detecting and deterring fraud and reducing shrink within their businesses.

Currently, fraud and abuse in the post-sale transaction process is an astronomical issue for retailers. A study performed by the National Retail Federation and Appriss Retail found that in 2023, the retail industry experienced approximately $743 billion in returns, with the total amount of dollars lost to abuse for fraudulent returns reaching an astonishing $101 billion.[1] This illustrates the need for Retailers to leverage fraud detection and deterrence software to help protect themselves from these losses.

Appriss Retail's "Engage" product considers the transaction history associated with a particular post-sale transaction request (such as a return, exchange, price adjustment or product not received claim) and evaluates the request for indicators of fraud or abuse. Based on the outcome of that evaluation, and depending on the Retailer's risk tolerance, Engage would recommend that the request would be denied, warned, or approved. In general, only 1% of post-sale transaction requests are denied as a result of Engage's analysis, but the potential loss to the Retailer for approving that 1% can be significant.

While the primary objective of this product is to help Retailers detect and deter fraud and abuse, this capability actually benefits the other 99% of the Retailer's customers.

First, when Retailers are able to review the transaction history associated with each post-sale transaction request for fraud or abuse, they are able to rely on that sophisticated process to reduce fraud and abuse related shrink while maintaining more flexible return, exchange, or post-sale adjustment policies and processes for vast majority of its customers.

Second, by leveraging software to evaluate a post-sale transaction request, Retailers are able to reduce the unconscious bias that may impact whether a particular consumer is permitted to return, exchange or receive a price adjustment. Historically, when a consumer needs to make a post-sale transaction request, they would go to the store or call the call center and speak with an employee. That employee would have the broad discretion on whether to approve or deny the request—relying on limited information available to them at the time in conjunction with the store's return, exchange or claim policies. Whether the employee is aware or not, their bias plays a factor in that evaluation. The consumer's race, age, ethnicity, dialect, or accent—are very likely to influence the employee's ultimate decision on whether to approve or deny the request. Our software strips the request process of bias by objectively evaluating each request based

---

1 https://cdn.nrf.com/sites/default/files/2024-01/2023%20Consumer%20Returns%20in%20the%20Retail%20Industry.pdf

solely on transactional data, such as number of returns, value of those returns, or purchase history.

Fraud can be as simple as an individual trying to return a stolen product or as complex as an Organized Crime Ring where multiple individuals work together to defraud a retailer. To further complicate things, experienced fraudsters are excellent at using fake names, email addresses, mailing addresses, etc. to effectuate their fraud. Even simplistic fraud schemes can be nearly impossible for a Retailer to detect without having immediate visibility to the complete transaction history associated with a request.

Providing consumers with the ability to access, correct, or delete their data, while beneficial in many ways, can have a detrimental effect on the Retailer's ability to detect fraud and abuse. Specifically, if a bad actor is able to demand the deletion of their transaction history, a retailer would have no ability to determine if the post-sale transaction request in front of them is valid or abusive. As such, Retailers would be forced to enact very strict post-sale transaction policies for all consumers to protect themselves against the potentially astronomical loss due to fraud or abuse.

In that same vein, allowing processors, like Appriss Retail, to analyze data received from all their Retailer customers holistically enhances the ability to detect fraud. For example, if a consumer has a history of wardrobing at one Retailer and begins to show that same behavior at a second Retailer, Appriss can identify and deter this fraudulent behavior quicker if we have visibility to the consumer's behavior in the first Retailer. This can save the Retailer significant losses, giving the Retailer the financial flexibility to provide consumers with legitimate post-sale transaction requests a frictionless experience.

Based on these concerns, we would propose two amendments to the current draft of the privacy bill:

First, we would request to make it clear that the exceptions outlined in the current section §2426 apply to the Consumer Personal Data Rights section §2418. This could be as simple as adding "unless an exception identified in §2426 of this Chapter applies," before listing the consumer data rights.

§2418 – Consumer Personal Data Rights

(a) Unless an exception identified in §2426 of this Chapter applies, a consumer shall have the right to:

Second, in the currently drafted §2421(9), which prohibits a processor from combining personal data obtained from multiple controllers, we would propose adding language that states that the processor may combine data in such a way if it is to perform the business purpose stated in the relevant data processing agreement or if the restriction would interfere with the processor or controller's ability to do one of the things that are exempted from this Chapter.

§2421 – Duties of Processors

> *(9) prohibit the processor from combining personal data obtained from the controller with personal data that the processor: (A) receives from or on behalf of another controller or person; or (B) collects from an individual, provided that the Processor may combine personal information: (i) to perform the business purpose as defined in the relevant agreement between the Controller and Processor, or (ii) if the restriction on combining data would restrict a controller's, processor's, or consumer health data controller's ability to do one or more of the identified purposes in 2426(a)(1)-(13).*

I've provided a written submission that includes proposed language and would welcome any questions you may have at this time. Thank you.