HB 3603
Is Too Overbroad to be Effective in its Current Form

Summary: As drafted, HB 3603 will not accomplish its goals of increased consumer protection, because consumers will receive so many opt-in consent notifications that the truly sensitive notifications will be rendered meaningless. The private right of action will be abused just as it has been in BIPA.

"Consumer Health Data" definition is too broad to be meaningful

- The current definition is so broad that it would include data about activities and purchases of goods that consumers use every day:
    - Purchasing toilet paper, deodorant, underwear, even shoes would be included – any data that related to "products that…affirm an individual's gender identity," or related to "bodily functions."
    - The location data element is so broad that it would include nearly any service that relies on location (for example, information used for good driver discounts, or that helps consumers find the nearest grocery store).
- A definition more precisely targeted toward data that Regulated Entities use to determine whether individuals have accessed reproductive or gender-affirming care services or information would better accomplish the goals of this legislation, avoiding significant unintended consequences and friction for consumers.

The breadth of "Consumer Health Data" definition will also prevent meaningful compliance

- By encompassing any data that "could be" – but is not necessarily – health related, the breadth of the definition creates an impossible obligation for companies by effectively establishing an opt-in regime for all collection of all data.
- Put simply, this definition encompasses virtually all data, *even if it was not intended to be used as health data at collection.*
- Because of the breadth and the impossibility of compliance, enforcement penalties will be unavoidable.

The legislation is well-intentioned but consumers will be confused by the current language

- There is no doubt that these subjects are sensitive, important, and top-of-mind for many Illinois residents. Consumers should know that their most sensitive data is being safeguarded and that they can provide or withdraw consent for particular activities.
- This legislation would be far more effective for consumers if normal, day-to-day transactions like purchasing hygienic products online or in retail locations could proceed uninterrupted. As drafted, the bill would require endless pop-up boxes or other

frustrating consent mechanisms that will interrupt normal consumer interactions. This will lead to consent fatigue and contravene the intent of the legislation.

Without changes to the definitions, many more changes will be necessary to treat this bill like a comprehensive privacy bill

- Without changes to narrow the scope of the bill, then the bill effectively becomes a comprehensive privacy bill, because nearly every piece of data could be "related to" health.
- Because of that, there would have to be significant additions to the bill that would align it with other states' privacy laws, including greater balance between consumer rights and operational necessities.
- Ultimately, narrowing the scope of the bill will allow consumers to exercise the greatest control over their most sensitive data.
    - For example, removing the term "biometric information" – which is not the focus of the bill – and adding a definition for "precise geolocation" – would help clarify the scope of what data would be regulated and focus on the data most susceptible to the type of activity the bill seeks to regulate.

The bill also lacks key definitions and provisions that can better protect consumers

- Terms in the bill that are key concepts remain undefined; adding definitions will help consumers and businesses better understand and effectuate the law's intent. Examples include:
    - Precise geolocation information
    - Process or Processing
- The bill should establish and allocate responsibilities of the parties according to role. For example, a cloud storage provider does not interact with consumers and thus will not be able to inform consumers of their rights.
- Much broader cybersecurity and anti-fraud provisions are also needed to close potential loopholes for bad actors. Businesses must be able to maintain high cybersecurity, authentication, and harassment protocols to prevent and mitigate identity theft and fraud.
- At the same time, the authentication requirements in this bill are overly prescriptive and inflexible.
    - As an example, other state privacy laws that provide consumer data rights such as Access and Deletion require the consumer to be authenticated prior to a business returning data to the requesting party in the context with which a business normally interacts with a consumer.

The Private Right of Action Will Not Help Consumers

- The Private Right of Action (PRA) in this bill will not provide the necessary protections to consumers; it will serve to create a cottage industry for the plaintiffs' bar, while providing minimal relief to consumers.
    - Studies have revealed that private rights of action fail to compensate consumers ***even when a violation has been shown***, and instead primarily benefit the plaintiff's bar by creating a "sue and settle" environment.[1]
- BIPA's PRA has not only failed to meaningfully protect consumers, but actually made them less safe, as companies that provide anti-fraud, convenient authentication, and other beneficial services leave the state because of abusive litigation risk.
- A recent Bloomberg investigation revealed a **65% increase in BIPA lawsuits since the *White Castle* decision**. Illinois should not repeat these mistakes with HB 3603.

[1] Mark Brennan et al., Ill-Suited: Private Rights of Action and Privacy Claims, U.S. Chamber Institute for Legal Reform (July 2019).