CAROLYN A. QUATTROCKI
Chief Deputy Attorney General

LEONARD J. HOWIE III
Deputy Attorney General

CARRIE J. WILLIAMS
Deputy Attorney General

SHARON S. MERRIWEATHER
Deputy Attorney General

ZENITA WICKHAM HURLEY
Deputy Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

ANTHONY G. BROWN
Attorney General

WILLIAM D. GRUHN
Division Chief

PHILIP ZIPERMAN
Deputy Division Chief

PETER V. BERNS
General Counsel

CHRISTIAN E. BARRERA
Chief of Staff

HANNA ABRAMS
Assistant Attorney General

February 17, 2026

TO: The Honorable Pamela Beidle, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 387 – Food Retailers – Dynamic Pricing, Surveillance Data, and Collective Bargaining Agreements (Protection from Predatory Pricing Act) SUPPORT WITH AMENDMENT

The Consumer Protection Division of the Office of the Attorney General supports the dynamic pricing and surveillance data provisions of Senate Bill 387 ("SB 387"), sponsored by President Ferguson, and Senators Augustine, Brooks, Charles, Harris, Hettleman, Kagan, King, Lam, Lewis Young, Love, and Zucker, with amendments. Senate Bill 387 limits the number of times a price may be changed in a given day and restricts the types of data that may be used to personalize prices in food retail establishments, thereby protecting consumers from these harms by reducing discriminatory pricing, curbing excessive data collection, and improving transparency in pricing practices.[1]

Specifically, SB 387 restricts food retailers' use of "surveillance data" and "dynamic pricing" to personalize prices for consumers. Both of these practices use massive amounts of data collected about an individual consumer to charge the highest price and extract the maximum profit that the consumer would be willing to pay for a given product or service. Companies exploit this trove of detailed personal data, or "surveillance data" – including, demographics, browsing history, location data, keystroke data, purchasing behavior, inferential data, and other data – to set the prices of goods and services on an individual basis. And consumers are often unaware that their data is even being collected. Similarly, "dynamic pricing" once referred to broad price adjustments based on market demand. Advances in data collection and real-time analytics now allow companies to change prices continuously, charging different consumers

[1] The Division's testimony is limited to the surveillance data and dynamic pricing provisions of SB 387.

different prices for the same product within minutes. When combined with electronic shelf labels, prices can be altered instantly based on time of day, weather, temporary events, or even inferred characteristics of the individual shopper.

"Dynamic pricing" and the use of "surveillance data" threaten consumer fairness by facilitating discriminatory pricing, encouraging invasive data collection, and obscuring prices, limiting consumers' ability to make informed choice. These practices are especially harmful in food retailers because food is an essential good, leaving households with little bargaining power or ability to avoid individualized price increases. By leveraging personal and behavioral data that correlate with income and vulnerability, such pricing disproportionately raises costs for those least able to pay while eroding privacy, trust, and the expectation of a fair, uniform price for necessities.

CPD Amendments

The Division recommends three amendments to SB 387 to clarify the scope and intent of the bill.

- Replace the phrase "personally identifiable information" in the definition of "surveillance data" (page 2, line 31 – page 3, line 4), with "personal data and publicly available information," cross-referencing the definition of "personal data" found in the Maryland Online Data Privacy Act (MODPA).[2] "Personally identifiable information" is not a term used in Maryland consumer protection law.[3] While it is found in the State Government Article, there it refers to a very limited number of pieces of consumer information such as a person's financial account number or driver's license.[4] In contrast, "personal data" encompasses the full scope of consumer personal data that is used in surveillance pricing.
- Replace the definition of "artificial intelligence"[5] (page 2, lines 15-16), with a cross reference to the Insurance Code's definition (MD Code Ann., Ins. Law, § 15-10B-05.1). As drafted, the definition fails to address two key aspects of artificial intelligence. By limiting its scope to "predictions, recommendations, or decisions" and omitting any reference to content, it may not clearly encompass systems whose primary function is content generation or other original outputs. Although content generation can be described technically as a form of prediction, that characterization is not apparent from the term's ordinary meaning. In addition, by restricting objectives to those that are "human-defined," the

[2] Md. Code Ann., Com. Law, § 14-4701(w) ("Personal data" means any information that is linked or can be reasonably linked to an identified or identifiable consumer).
[3] The Maryland Personal Information Protection Act uses the term "personal information" (Md. Code Ann., Com. Law, § 14-3501(e)), and the Maryland Online Data Privacy Act uses "personal data" (Md. Code Ann., Com. Law, § 14-4701(w)).
[4] Md. Code Ann., State Gov't, § 10-13A-01(f).
[5] Md. Code Ann., State Fin. And Proc. § 3.5–801 reads: (c) "Artificial intelligence" means a machine–based system that: (1) can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments; (2) uses machine and human–based inputs to perceive real and virtual environments and abstracts those perceptions into models through analysis in an automated manner; and (3) uses model inference to formulate options for information or action.

definition does not clearly encompass implicit objectives—goals not explicitly coded but learned from data or inferred from behavior. The definition found in the Insurance Code provides sufficient flexibility to accommodate both existing technology and future developments.

- Limit the store loyalty program exemption. On the surface, loyalty rewards programs entice consumers by offering free enrollment accompanied by discounts. In reality, loyalty programs function as "surveillance infrastructure": consumers often unknowingly pay for this benefit with their personal data.[6] A Consumer Reports investigation revealed that Kroger collects such vast amounts of data to build profiles of its customers that one profile stretched across *62 pages* and included inferences about the consumer's income, gender, household size, and education.[7] Rather than benefiting consumers, Kroger has monetized this information, reportedly selling or sharing these loyalty profiles with more than 50 companies, from tobacco firms to data brokers to health tech companies, making more than 35% of the company's net income in 2024 from leveraging this data.[8]

The Division asks the Senate Finance Committee to issue a favorable report with the amendments discussed.

Cc: Governor Wes Moore
President Bill Ferguson
Senator Malcolm Augustine
Senator Benjamin Brooks
Senator Nick Charles
Senator Kevin M. Harris
Senator Shelly Hettleman
Senator Cheryl C. Kagan
Senator Nancy J. King
Senator Clarence K. Lam
Senator Karen Lewis Young
Senator Sara Love
Senator Craig J. Zucker
Members, Finance Committee

[6] Samuel A.A. Levine and Stephanie T. Nguyen, "The Loyalty Trap: How Loyalty Programs Hook Us with Deals, Hack Our Brains, and Hike Our Prices", Vanderbilt Policy Accelerator (October 2025).
[7] *See* Cyrus Rassool, "Consumer Reports Investigation Uncovers Kroger's Widespread Data Collection of Loyalty Program Members to Create Secret Shopper Profiles," CONSUMER REPORTS (May 21, 2025), https://www.consumerreports.org/media-room/press-releases/2025/05/consumer-reports-investigation-uncovers-krogers-widespread-data-collection-of-loyalty-program-members-to-create-secret-shopper-profiles/
[8] *Id*.