



Consumer Data Industry Association  
1090 Vermont Ave., NW, Suite 200  
Washington, D.C. 20005-4905

April 8, 2026

P 202 371 0910

[CDIAONLINE.ORG](http://CDIAONLINE.ORG)

Representative Carol Hagan McEntee  
Chair  
House Committee on Judiciary  
Rhode Island General Assembly  
82 Smith Street  
Providence, RI 02903

Chair McEntee and Members of the Committee:

On behalf of the Consumer Data Industry Association (CDIA), I write to express our continued concerns regarding unintended consequences of broad provisions in Rhode Island's Judicial Security Act and encourage the committee to consider adopting our previously proposed amendments to the underlying statute as part of H7640. CDIA supports the intent of the Judicial Security Act and as we have in other states, stands ready to work with the committee and Courts to improve the bill and underlying statutes by addressing the concerns outlined below. We believe it is important to establish strong pathways to protect sensitive information of protected individuals without disrupting the important work of our industry to protect all consumers.

CDIA is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals, and to help businesses, governments and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity, helping ensure fair and safe transactions for consumers, facilitating competition and expanding consumers' access to financial and other products suited to their unique needs.

CDIA recognizes, appreciates, and supports the intent of the bill to keep the personal information of protected individuals from being made available to the public. While our members work with this information for a variety of legitimate business purposes like credit reporting, background checks, tenant screening, identify verification, fraud detection, or vehicle recalls, the information is not made available to the public. However, as the definition of data aggregator broadly captures our members and the scope remains so broad, the bill risks disruption to these legitimate business activities that benefit the members of the protected class.

H7640 would amend (c)(6) to allow authorized agents to submit written requests to persons, data aggregators, businesses, or associations to effectuate the prohibition on any transfer of personally identifiable information. While this aligns (c)(6) with (c)(3), inconsistencies remain that make compliance challenging and risk unintentionally disrupting data uses that benefit the protected individuals. The broad restrictions retained in (c)(1) and (c)(6) do not distinguish between making the protected information of a protected individual available to the general public or using it for legitimate business activities that may be regulated by one or more federal privacy statutes like the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), or the Driver's Privacy Protection Act (DPPA), among others.

This risk increases in light of the covered persons' ability to allow authorized agents to make requests, as those entities may not fully understand what types of databases they are seeking to have the covered persons' information deleted from and thus may not be able to fully inform the covered person of the unintended consequences until it is too late. As a result of how the law is structured, once the information

is deleted from these databases, it cannot be recovered, which is particularly concerning in the context of consumer reporting, identity verification, and safety recall uses.

While CDIA appreciates the intent of (c)(5) to require authorized agents provide an affidavit from the protected individual, we would respectfully request clearer verification procedures to authenticate the individuals who are making the requests. Without a strong verification mechanism in place, companies can have difficulty identifying and processing legitimate requests within the law's 10-day compliance window. This potentially exposes companies to frivolous lawsuits because of the difficulty in verifying the identity of the protected class.

CDIA acknowledges the intent of the underlying statute and the proposed changes in H7640 to ensure the efficacy of pathways by which public servants can protect their sensitive personal information from being accessed by the public in a manner that could put them or their loved ones at risk. We are proud of our work across the country to work with state legislatures to craft similar statutes that protect information without unintended consequences. We respectfully request that H7640 be amended to reflect CDIA's previous requests to clarify the scope and intent of the statute, avoiding unnecessary disruption to our members' business operations that support a variety of beneficial activities. Thank you for your time and consideration.

Sincerely,



Sarah Ohs  
Vice President, Government Relations  
Consumer Data Industry Association