In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
	)	

Reply Comments of Consumer Choice Center

The Consumer Choice Center is grateful to the Federal Communications Commission for their interest in exploring this important topic of Robocalls further. Protecting consumers from illegal robocalls and scams in our telecommunications network is an important function of the FCC.

We feel it is important to note that, as the Commission already notes in its notice, they already have Know Your Customer (KYC) rules on the books. It's critical to start from the premise that if the Commission feels that providers are not doing enough, that is a matter of enforcing the existing laws and regulations rather than creating a more onerous, and potentially invasive set of new requirements on businesses.

Emerging technologies like Artificial Intelligence can help businesses meet their existing obligations. However, the Commission should encourage technologically neutral tools for businesses to leverage and be in compliance rather than prescribing into regulation a single technological solution to the underlying issue.

We also feel it's important for the Commission to proceed cautiously before seeking to expand KYC requirements into a broad information collection exercise. Simply requiring businesses to collect more data does not necessarily mean that consumers will be better protected as a result of those efforts. In fact, the opposite can be true: imposing such mandates creates privacy and cybersecurity risks in the process.

While protecting consumers is a key function of a regulator, it's critical for regulators to understand the risks of adopting such broad expansions to policies that can lead to adverse outcomes that threaten the civil liberties of Americans, and by extension, their trust in the systems that are charged with keeping them safe.
For example, in the notice, the Commission points to the BSA and the Customer Identification Portal (CIP) rules as a potential model for the agency to follow. However, we feel the FCC should avoid replicating the BSA and its requirements. The

rigid KYC requirements of the BSA should serve as a cautionary tale. Not only are the requirements a massive compliance cost put on businesses with a serious issue of false positive rates. The increased compliance costs are ultimately passed down onto consumers.

Mandating that carriers gather, authenticate, and retain government identification, residential addresses, and additional sensitive information for four-years makes voice providers into lucrative marks for malicious actors. Considering the industry's struggles resulting in security failures, a regulatory requirement potentially creating a centralized warehousing of sensitive personal data simply to activate basic services subjects millions of citizens to unnecessary identity theft vulnerabilities.

Tackling illegal calls effectively without negatively impacting consumers and stifling technological innovation is important. The Commission should focus on enforcing existing rules, utilize a flexible safe harbor regime that rewards the positive outcome, and avoid turning our service providers into quasi communication surveillance agencies more than they already are under other laws. The FCC should avoid replicating the costly and privacy invasive nature of the BSA format.

Sincerely,

James Czerniawski

Head of Emerging Technology Policy

Consumer Choice Center

The Consumer Choice Center is an independent, non-partisan consumer advocacy group championing the benefits of freedom of choice, innovation, and abundance in everyday life.