Before the
Federal Communications Commission
Washington, D.C. 20554

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

COMMENTS
OF
NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION & SUMMARY

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these comments in response to the Further Notice of Proposed Rulemaking released by the Federal Communications Commission ("Commission") in the above-captioned proceedings.[2] The Commission seeks comment on enhancing existing "Know-Your-Customer" ("KYC") provisions that require Originating Service Providers ("OSPs") to "[t]ake affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls."[3] NTCA supports the Commission's efforts to eliminate the scourge of illegal robocalls as well as "spoofing" enabled scams that harass and victimize consumers. When combined with other measures, KYC

[1] NTCA is an industry association composed of approximately 850 community-based companies and cooperatives that provide advanced communications services in rural America and more than 400 other firms that support or themselves are engaged in the provision of such services. As a founding member of the Secure Telephone Identity Governance Authority ("STI-GA") Board of Directors, NTCA has put its members' commitment to protecting rural consumers and combatting the scourge of caller-ID spoofing into action with time and financial resources dedicated to the creation of the STI-GA.

[2] *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, Further Notice of Proposed Rulemaking, FCC 26-27 (rel. May 1, 2026) ("*Further Notice*").

[3] *Id*., ¶ 6, citing 47 CFR § 64.1200(n)(4).

requirements can be an effective "tool in the toolkit" to combat these calls. However, the Commission should narrowly tailor any subscriber identity verification requirements it adopts via this proceeding to avoid (i) unnecessary burdens on smaller operators with limited financial resources and (ii) overly intrusive processes that will frustrate consumers. More specifically, the Commission should establish a risk-based approach to KYC requirements and adopt a baseline set of KYC practices that, if followed by OSPs, acts as a "safe harbor" for enforcement purposes.

II. A RISK-BASED APPROACH TO "KNOW YOUR CUSTOMER" RULES WOULD TARGET THE MOST LIKELY BAD ACTORS WHILE AVOIDING UNNECESSARY BURDENS FOR SMALL PROVIDERS.

A. Overly broad Know Your Customer rules would impose needless burdens on small providers.

The Commission should narrowly target any rules to target the bad actors involved in creating and distributing robocalls, not the small business owners and Americans living in rural communities. As the backdrop to this discussion, NTCA members operate in difficult to serve rural areas of the nation, where topography, distance from urban centers, and typical densities of fewer than seven locations per mile drive up the cost to build and operate voice and broadband networks. These providers serve on average 6,000 broadband subscribers and 3,000 voice subscribers, and do so with an average of 30 total employees.[4] Regulatory compliance costs strain these providers' resources and, critically, must be recovered from a small, rural customer

[4] *NTCA Broadband Internet Availability Survey 2025*, (rel. Dec. 2025), pp. 2-4, *available at* https://www.ntca.org/sites/default/files/documents/2025-12/2025BroadbandInternetAvailabilityReport.pdf.

base. Moreover, in recent years, STIR/SHAKEN,[5] robocall mitigation,[6] and call blocking mandates[7] from the Commission have driven up these compliance costs.

To be clear, as community-based providers, NTCA members take seriously their duty to provide trustworthy and reliable communications services to rural Americans, and they are committed to utilizing every tool they can to mitigate the problem of unwanted calls received by their subscribers. NTCA members' executives and other staff live in the communities they serve, and they therefore hear first-hand complaints about problematic robocalls from their neighbors. In service of that commitment, NTCA has been supportive of the Commission's action to clarify voice providers' legal authority to block unwanted or illegal calls,[8] has actively worked to adopt call authentication solutions to combat caller-ID spoofing for "non-IP" networks,[9] has urged the Commission to require providers' use of these solutions,[10] has actively

[5] *Call Authentication Trust Anchor*, Second Report and Order, WC Docket No. 17-97, FCC 20-136 (rel. Oct. 1, 2020), ¶ 40 (requiring small providers – defined as those with 100,000 or fewer voice subscriber lines – to implement call authentication technology by June 2023).

[6] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (rel. Mar. 17, 2023), ¶ 3 (adopting expanded "robocall mitigation requirements for all providers").

[7] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Eighth Report and Order, FCC 25-15 (rel. Feb. 28, 2025), ¶ 1 (expanding the "requirement to block calls based on a reasonable do-not-originate (DNO) list" and establishing "SIP code 603+ as the exclusive code to notify callers when calls on Internet Protocol (IP) networks are blocked based on reasonable analytics to better correct erroneous blocking.").

[8] Comments of NTCA, CG Docket No. 17-59, WC Docket No. 17-97 (fil. Aug. 9, 2023), p. 3.

[9] NTCA has served on the Alliance for Telecommunication Industry Solutions Non-IP Call Authentication Task Force since its inception.

[10] Comments of NTCA, WC Docket No. 17-97 (fil. Jul. 16, 2025), pp. 2-5.

worked to advance the IP transition to ensure spoofing mitigation technology functions as intended,[11] and has supported robocall mitigation practices.[12]

As the Commission considers KYC rules, NTCA strongly urges the agency to address the source of most if not all illegal robocalls. The Commission should avoid burdensome provisions that are also likely to be ineffective and/or unnecessary. As described below, individual residential subscribers as well as small businesses are unlikely to be the source of these unwanted calls, and subscriber identity verification processes directed as these callers will impose compliance costs on OSPs unnecessarily. This would divert resources from more effective efforts to address illegal robocalls and again, for small rural OSPs, force these costs to be recovered from a small customer base.

B. Burdensome rules are unnecessary considering the numerous other steps that providers undertake to address the scourge of illegal robocalls.

The Commission's approach to KYC provisions should be informed by the many other tools in the toolkit that OSPs use to address these unwanted calls. In particular, robocall mitigation practices are a powerful tool to stop large-scale robocalling patterns in their tracks. The fact that OSPs must engage in effective mitigation practices or have all of their traffic blocked is an incredibly strong incentive for them to take these obligations seriously. STIR/SHAKEN call authentication technology, call blocking tools (driven by data analytics) and the Industry Traceback Group that has proven itself able to rapidly identify the source of illegal robocalls[13] all work together to address this problem. Evidence has shown that so far, small

[11] Comments of NTCA, WC Docket Nos. 25-208, 25-209, 17-97 (fil. Jan. 20, 2026), p .19

[12] Comments of NTCA-The Rural Broadband Association, WC Docket No. 24-213, MD Docket No. 10-234 (fil. Oct. 15, 2024), p. 1.

[13] *See* Letter from Joshua M. Bercu, Executive Director, Industry Traceback Group to Marlene Dortch, Secretary, Federal Communications Commission, RE Enforcement Bureau Requests Information on the

RLECs are not the cause. Thus, while KYC rules are a helpful tool, they are only one part of the puzzle. A limited KYC rule, in combination with the other tools described in these comments, can be highly effective when targeted to the likely source of illegal calls. Importantly, a limited KYC rule would also avoid unnecessarily burdening providers and frustrating consumers with legitimate privacy concerns.

C. Any rule should be appropriately tailored to address the callers most likely to engage in large scale illegal robocall campaigns.

The Commission should adopt a risk-based approach to KYC rules that allows providers to target subscriber vetting practices toward entities seeking access to high-volume call origination and similar services.[14] As an initial matter, as the Call Authentication Trust Anchor Working Group found, "[r]esidential and small business retail End-Users (i.e., mass market Customers) present a low risk for perpetrating illegal robocalls. [Voice Service Providers] collect End-User address contact information for general provisioning and billing of service."[15] Additional subscriber vetting at the retail and small business level is therefore likely to be ineffective and worse unnecessary, directing providers' time and financial resources away from the more likely sources of illegal robocalls.

Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls, EB Docket No. 20-195, DA 25-261 (fil. May 1, 2025).

[14] *Further Notice*, ¶ 13 ("Should we require originating providers to collect more information about customers that are more likely to make illegal calls, e.g., those subscribing to high volume services or those that may be difficult to locate based on being foreign-based, or other factors?").

[15] *Best Practices for the Implementation of Call Authentication Frameworks*, NANC Call Authentication Trust Anchor Working Group (rel. Sep 24, 2020), p. 9 available at: https://www.fcc.gov/document/best-practices-implementation-call-authentication-framework. The report went on to state that "[r]etail End-User service is generally provisioned to a fixed location, is easily identifiable, and is unlikely to generate illegal robocalls." *Id*.

In addition, as Commissioner Gomez highlighted, residential and small business subscribers are likely to balk at the privacy implications raised by KYC measures directed at them.[16] Obtrusive measures such as those proposed in the *Further Notice* include not only additional vetting/proof of identity and a requirement to provide documentation before service is initiated but also OSPs' retention of that documentation. The record is replete with individual consumer comments filed in response to the *Further Notice* that indicate that many Americans will be frustrated by the intrusive nature of unnecessary additional vetting procedures, and are wary of the privacy implications.[17]

Thus, to address these consumer privacy concerns while attacking the true bad actors, the Commission should first adopt baseline KYC processes that all OSPs should undertake with respect to the provision of high-volume call origination services only.[18] Similar to those adopted

[16] Statement of Commissioner Anna Gomez, *Call Authentication Trust Anchor; Advanced Methods to Target and Eliminate Unlawful Robocalls, Further Notice of Proposed Rulemaking*, WC Docket No. 17-97; CG Docket No. 17-59 (May 20, 2026) ("But as we strengthen these rules, we must also be clear about who they're aimed at. After we voted on the Know Your Customer robocall NPRM last month, I noticed growing bipartisan concern online about what these new vetting requirements would mean for the privacy of everyday consumers. People wanted to know whether buying a prepaid phone or activating a prepaid line would require, for the first time, government-issued ID. That concern is understandable and it deserves a clear answer. As the Commission's robocall enforcement efforts expand across authentication, numbering, and provider accountability, we have an obligation to be clear that these rules target the business relationships between carriers and should not erode consumer privacy.").

[17] *See e.g.* Express Comment of Molly C, CG Docket Nos. 17-59, 02-278 (fil. Jun. 18, 2026) ("Collecting personally identifiable information when a person purchases a new phone or renews a contract is not an effective way to combat the scourge of robocalls. This measure would, however, curb privacy protections. Please retract this proposed rule."). Several similar express comments have been filed.

[18] The Commission should define "high-volume call origination services" as it did in the *Lingo Telecom Consent Decree*. *Lingo Telecom, LLC*, File No.: EB-TCD-24-00036425, NAL/Acct. No.: 202432170004, FRN: 0035440734, Order, DA 24-790 (rel. Aug. 21, 2024), Attachment 1: Operating Procedures (*Lingo Telecom Consent Decree*") (defining a "SIP Trunking Product" as "a single connection comprised of multiple communications channels that provides Voice over Internet Protocol connectivity between an on-premise phone system and the public switched telephone network.").

in the *Lingo Telecom Consent Decree*,[19] OSPs should collect data such as company name, address, Tax Identification Number, and Business Registration Number, verified through a reputable third-party entity.

This risk-based approach should also recognize that OSPs need the flexibility to at times take additional steps beyond those set forth in baseline requirements with respect to subscriber vetting – including for high-volume services users as well as business customers – based upon the evolving tactics that bad actors will employ. A static set of requirements is likely to soon be outdated as those entities determined to continue making illegal robocalls will change their tactics accordingly. Thus, a baseline set of requirements as proposed above, supplemented by additional steps that OSPs determine on their own are necessary to respond to changing tactics they see as they monitor traffic patterns via their robocall mitigation practices, strikes the appropriate balance.

Any rules must provide OSPs the flexibility to supplement baseline requirements and use the right tools in the toolkit to respond to the unique characteristics of an illegal robocall campaign. Offering providers the flexibility to direct resources at the most likely source of illegal robocalling campaigns while avoiding deploying limited resources aimed at subscribers that present little to no risk of placing these calls is the most effective way to limit illegal calls.

D. The Commission should adopt baseline Know Your Customer requirements that operate as a regulatory safe harbor.

Any KYC framework that permits compliance with the baseline requirements proposed above should operate as a safe harbor for enforcement purposes. As an initial matter, the $2,500 per call base forfeiture amount proposed in the *Further Notice* could quickly outpace the

[19] *Id*.

resources of a smaller provider if not push them into outright bankruptcy. Forfeiture amounts at the level proposed in the *Further Notice* should be reserved for entities that brazenly flout the Commission's rules or fail to cooperate with traceback requests.

A safe harbor, on the other hand, would grant OSPs the flexibility to apply the baseline procedures to the entities that pose the most risk of engaging in large scale illegal robocall campaigns and to take additional verifications steps where those may be warranted.

III. CONCLUSION

For the reasons set forth above, the Commission should adopt a risk-based approach to KYC with a baseline set of practices that operate as an enforcement safe harbor.

Respectfully submitted,

By: /s/ Justin Faulb
Justin Faulb
Senior Vice President – Policy and
General Counsel

By: /s/ Brian Ford
Brian Ford
Vice President – Federal Regulatory

4121 Wilson Boulevard
Suite 1000
Arlington, VA 22203
703-351-2000 (Tel)

June 25, 2026