**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 THE VOICE ON THE NET COALITION**

The Voice on the Net ("VON") Coalition[1] hereby submits these comments in response to the Further Notice of Proposed Rulemaking (the "FNPRM") in the above-referenced dockets.[2] VON supports the Commission's goal to deter illegal calls and urges adoption of a flexible, competitively neutral, innovation-friendly, and risk-based Know Your Customer ("KYC") safe harbor approach that reflects the diversity of services and customer bases in the market, as well as industry best practices. KYC policies are one aspect of effective fraud prevention, and are best developed and implemented along with monitoring, traceback, and authentication tools.

## I. BACKGROUND

VON members are interconnected VoIP providers offering enterprise Unified Communications as a Service ("UCaaS") and Contact Center as a Service ("CCaaS") solutions to a diverse customer base, including home-based sole proprietors and small businesses, large

[1] The VON Coalition works to advance regulatory policies that enable Americans to take advantage of the promise and potential of internet communications. See www.von.org.
[2] *Further Notice of Proposed Rulemaking,* CG Docket Nos. 17-59 and 02-278 (rel. May 1, 2026); see also 91 Fed. Reg. 30596 (May 26, 2026) (establishing a comment deadline of June 25, 2026).

enterprises and government agencies, and legitimate high-volume contact centers. VON's interest is ensuring effective, scalable KYC protocols that protect consumers and networks without chilling lawful communications or imposing unworkable mandates.

## II. Overarching Principles

As the Commission considers the path forward in this proceeding, and as discussed more fully below, VON recommends that the decision align with the following principles**:**

1. **Industry-wide technology neutrality.** Must be practical, common-sense, scalable, and technology-neutral and apply uniformly across the industry without mandating proprietary tools or vendor-specific solutions.
2. **Tiered and flexible compliance.** Must allow providers to scale their practices based on customer risk profiles and business models—from residential/work from home sole proprietors to high-volume contact centers.
3. **Baseline Information and Safe Harbor.** Must establish clear, objective compliance baselines and safe harbors.
4. **Flexibility in vetting.** Must not require use of "qualified third parties" or proprietary platforms as a condition of compliance.
5. **Proportionate enforcement**. Must not impose per-call KYC penalties and recognize good-faith compliance, safe harbor adherence, and prompt remediation.

## III. Customer Identification Requirements

VON supports a requirement to collect baseline KYC information from new customers, while allowing providers flexibility to require additional information from customers based on risk

profiles. Baseline customer information requirements should include: : name, physical address, government-issued identification number (for entities, an EIN or business registration where applicable), and an alternate telephone number or email address.

In terms of specifics, the Commission should define "physical address" to include valid commercial or residential locations. Rather than categorical exclusions, higher risk scenarios, such as virtual maildrops or other provider-identified scenarios, should be flagged for enhanced checks.

For higher risk use cases, providers should be permitted—but not required—to collect additional elements (e.g., intended use, business presence evidence) based on risk triggers rather than across-the-board expansion

**IV. High-Volume and High Risk Tiering**

The Commission should adopt a flexible framework and provide technology-neutral examples to guide "high-volume" determinations, allowing providers to set context-appropriate thresholds by service type and typical usage, consistent with prior flexible treatment.

The Commission should avoid adopting draconian regulations that chill protected speech and impede legitimate use cases. The Commission should not equate volume with risk per se; but allow VSPs to use contextual indicators, such as traffic analytics tuned to distinguish legitimate high-volume or intermittent calling behavior from abusive patterns and evolving AI monitoring tools, and remediation pathways before denying customer access or terminating an existing customer.

For higher risk customers, providers should be allowed to develop their own internal risk profiles and may decide to collect additional information such as business registration information, proof of commercial presence, and intended uses of the service, as appropriate. The Commission should not require providers to collect customer IP addresses from which each call will be made, which would be inconsistent with the modern hybrid work environment and 21st century travel habits. Customer's IP addresses will change any time they move locations (e.g., from the office to home) or travel for work, and it would be impractical to collect and verify each IP address. In addition, as more internet service providers rely on dynamic IP addresses, the IP address may not be a reliable indicator of a caller's location or identity

The Commission should not assume that foreign-caller use cases are per se high risk. Many of these use cases are legitimate, such as providing customer support to U.S.-based customers. Providers should have flexibility to determine risk profiles and require enhanced measures where needed. Regarding proposed requirements to check various lists, VSPs already comply with sanctions screening to prevent illicit transactions by prohibited entities, individuals, including those from countries designated as foreign adversary nations. These lists are maintained by the US Treasury's Office of Foreign Assets Control[3] and the Commerce Department's Bureau of Industry and Security Denied Persons List.[4] Any added list checks should be optional or risk-triggered, harmonized with existing compliance programs, and technology-neutral.

[3] See: https://sanctionssearch.ofac.treas.gov/.
[4] https://www.bis.gov/licensing/end-user-guidance/denied-persons-list-dpl.

**V. Verification and Re-Verification**

The Commission should encourage layered verification options. This would permit multiple pathways—documentary (e.g., government issued IDs, business registrations) and non-documentary (e.g., commercial databases, public records, reference checks, direct customer contact)—with staged activation that allows low-risk services to begin while enhanced steps are completed for high-risk functions. The Commission should not require mandatory third-party vetting or proprietary solutions. Such mandates would create bottlenecks, increase costs and onboarding delays, and expand sensitive data exposure without demonstrable benefits over provider-controlled, risk-based methods.

VON opposes a categorical requirement to re-verify customers upon renewal, including automatic renewals. Uniform periodic re-verification would harm consumers and legitimate businesses, with limited marginal benefit compared to effective traffic monitoring and red-flag triggers already contemplated by the FNPRM. For example, elderly American consumers may not be able to easily comply with recurring verification requirements and would risk losing access to phone service, including emergency 911 service, for non-compliance. In the business context, legitimate small businesses would bear the cost of submitting reverification materials in perpetuity and could risk losing business income if they lose phone service, even if temporarily, due to an administrative oversight.

Instead, VON recommends risk-based, not calendar-based re-verification of customer identification. Active network monitoring, in compliance with Section 64.1200(n), and reverification triggered by internal network alarms are the most effective way to catch bad actors and remove them from the phone network. Re-verification should only be triggered if a provider

actively detects suspicious activity or network red flags.

**VI. Treatment of Resellers, Intermediaries, and Complex Enterprises**

Any new KYC rules should require VSPs to verify their direct customers, including complex enterprises, and VSPs' resellers, brokers, agents, and other intermediaries before giving customers' or resellers' end customers access to phone numbers for voice calls. VON does not recommend different rules for verifying complex enterprises. KYC requirements that apply to corporate customers should apply evenly both to single corporations and complex enterprises. VSPs should not be categorically required to perform KYC on the end-customers of VSPs' resellers. Instead, VSPs should be allowed to obtain reasonable assurances/contractual commitments from the parties that have the ultimate relationship with the end customer that the third party performed legally-required KYC.

**VII. Compliance Timelines**

Regarding implementation timelines, VON recommends that the Commission apply new rules prospectively to new customers after a reasonable implementation period (e.g., 12 months after OMB approval of the new requirements). Changes to existing KYC processes will require time to plan and execute any necessary engineering changes, as well as to educate customers on new requirements. The Commission should also align any new requirements adopted in this proceeding with existing and proposed regulations regarding KYC, KYC Upstream Provider, numbering caller identity and offshore call centers to minimize duplication and cost.

**VIII. Safe Harbors and Use of Technology**

The Commission should establish a clear safe harbor such that VSPs that implement defined baseline KYC processes (core dataset, risk-based verification options, red-flag re-verification, retention and security controls) are deemed in compliance absent evidence of willful misconduct and would not be subject to violations of 47 CFR 64.1200(n)(4). Safe harbors will encourage broad industry compliance without fear of protracted enforcement proceedings and will also hopefully deter frivolous private action or class action lawsuits. Safe harbors should be technology neutral, keyed to outcomes and documented processes, and not specific tools. Moreover, while use of third parties may be permissible as one option it should neither be required nor the sole basis of safe harbor eligibility, and use of similarly robust internal tools should carry equal weight.

**IX. Enforcement Framework**

VON opposes the proposed $2,500 per-call base forfeiture for KYC violations. It is disproportionate in high-volume UCaaS/CCaaS contexts and risks existential liability for administrative errors. The Commission should instead assess penalties per-account or per-infraction, considering safe harbor adherence and remediation speed. At a minimum, any per-call penalty should be limited to calls that resulted in actual fraud or deception, not every single call placed on a provider's network during a period of deemed non-compliance.

The Commission should also avoid adopting new standalone certification obligations. Any additional certifications should be integrated into existing Robocall Mitigation Database recertifications without duplication, with clear notice and an opportunity to cure. Additionally, the Commission should not allow for downstream blocking tied to provider-judged KYC non-

compliance. Existing FCC rules already allow for or require blocking in defined scenarios, such as failing to appear in the RMD database, and increasing provider discretion to block traffic will result in blocking legitimate calls and increase the likelihood of anticompetitive conduct.

Providers should not, and cannot, be required to provide customer information to law enforcement or the Commission in the absence of a lawful order compelling the provider to do so. There are existing laws in this space that both the Commission and providers must adhere to.

**X. Ensure any new rules preserve and enhance competitive neutrality**

The Commission should not require adoption of proprietary solutions or allow for industry-mandated KYC obligations, which have proven to be ineffective at preventing fraud, involve inaccuracies that interfere with legitimate calls, delay service initiation, and harm competition in the communications marketplace, to the detriment of consumers, innovators, and small businesses. For example, where providers rely on analytics companies to make decisions on blocking traffic or labeling traffic as "likely fraud", such arrangements have repeatedly led to blocking and mislabeling legitimate traffic, with disparate impacts on competitive providers.

Whitelisting numbers can also lead to similar distortions when gatekeepers require competitive providers to share customer or phone number lists and require payment to prevent blocking or mislabeling. This approach effectively raises the cost for competitive providers and creates an unlevel playing field when the gatekeepers do not impose similar costs and threats of blocking or mislabeling upon themselves or their own customers.

## CONCLUSION

As discussed herein, VON urges the Commission to adopt technology-neutral, industry-wide, risk-based KYC standards with clear safe harbors and proportional, administrable enforcement. These steps will strengthen protections against illegal calls while preserving innovation, competition, and lawful, high-volume communications.

Respectfully submitted,

**VOICE ON THE NET COALITION**

*/s/ Glenn S. Richards*
Glenn S. Richards
Dickinson Wright PLLC
1825 Eye Street, NW, Suite 900
Washington, DC 20006
(202) 466-5954
grichards@dickinson-wright.com

Its attorney

June 25, 2026