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
Call Authentication Trust Anchor	)	WC Docket No. 17-97

REPLY COMMENTS OF THE VOICE ON THE NET COALITION

The Voice on the Net ("VON") Coalition[1] hereby submits this reply in response to comments filed in the Further Notice of Proposed Rulemaking ("FNPRM") in the above-referenced dockets.[2] There is much industry agreement that the Commission should adopt a flexible, risk-based know-your-upstream provider ("KYUP") provider framework, avoid any strict or disproportionate liability, and codify the STIR/SHAKEN attestation standards without shifting its regulatory authority to the STI/GA or to the marketplace generally. VON submits this reply to raise concerns about certain commenters' pushing the Commission to adopt rules to benefit the commercial interest of certain entities and re-iterate that the best way to retain visibility in the call flow is to allow initiating providers to continue to sign voice calls.

---

[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 No. 17-59 and WC Docket No. 17-97 (rel. May 21, 2026); see also 91 Fed. Reg. 42602 (July 9, 2026) (establishing a reply comment deadline of September 8, 2026).

DISCUSSION

A. The Commission should not adopt rules that go beyond the targeted problem.

While the VON Coalition supports the Commission's efforts to combat fraud and scams at all points in the call path, overly prescriptive and inflexible rules will create significant administrative burdens without addressing the root causes of illegal traffic.[3] To this end, VON has supported reasonable and actionable know-your-customer ("KYC"),[4] KYUP[5] and caller identity[6] rules that will (1) provide VSPs the flexibility necessary to tailor mitigation strategies to their unique networks and customer use cases and (2) encourage innovative mitigation strategies to address new and evolving threats without (3) converting one vendor's commercial model into the architecture of a federally mandated trust regime. While Numeracle's experience may contribute usefully to the record, its main interest here is not to protect the American consumer but to increase the economic reach of its vetting models. VSPs should be able to select a KYUP verification model that best fits its needs and customer base and not be tied to any third-party's proprietary software. To that end, VON reiterates that any framework should remain technology-neutral, competitively neutral, and not impose onerous or unnecessary record retention obligations.

Indeed, commercial verification services have incentives to: Expand the information providers must verify (including those that are not relevant to the service), increase the frequency

[3] A more effective approach would be for the Commission to use its existing enforcement authority to target the small number of VSPs (less than 50) that are responsible for most of the illegal calls. The Commission should not be swayed by comments that recommend the adoption of burdensome regulations that portend to hold all VSPs responsible for the sins of the few. See, e.g., Comments of Numeracle, Inc., WC Docket No. 17-97 (filed August 10, 2026) at 5-8.
[4] See, Comments of the Voice on the Net Coalition, CG Docket No. 17-59 (filed June 25, 2026).
[5] See, Comments of the Voice on the Net Coalition, CG Docket No. 17-59 (filed August 10, 2026).
[6] See, Comments of the Voice on the Net Coalition, CG Docket No. 17-59 (filed January 5, 2026).

of reverification, encourage rules that make the purchase of third-party services preferable or necessary, bundle verification with monitoring, reputation management, call treatment, or branding, and promote reliance on proprietary data or scoring methodologies.

For similar reasons, VON posits that any audit requirement should only be imposed when the Commission has objective evidence of non-compliance and a documented reason to require such audit. It should be triggered by objective Commission findings or clearly defined criteria, not proprietary reputation scores, disputed analytics, or unverified allegations. In addition, an audit should be conducted by an independent third-party, not commercial verification providers or analytics engines.

There is a role for commercial verification services for those VSPs that may require them. A commercial verification service should be able to confirm objective facts such as legal existence, business registration, physical address, identity of identified principals, and Robocall Mitigation Database ("RMD") and FCC Form 499 filing status. Likewise, VSPs should have flexibility to rely upon a variety of sources and tools to obtain objective facts, including internal resources.

When it comes to confirming regulatory status and the right to participate in the voice ecosystem, however, the RMD is the most appropriate central source. The majority of commenters recognize the importance of filings in the RMD and FCC enforcement as the appropriate regulatory foundation. VSPs are well-aware of the Commission's enforcement authority, including recent pronouncements citing companies for allegedly facilitating illegal robocall traffic and failing to respond to traceback requests.[7] Robocall-related enforcement

[7] See, Letter from Patrick Webre, Chief FCC Enforcement Bureau, to Leonardus Herps, CEO, RGTN USA, Inc., released August 24, 2026 (notifying RGTN of suspected illegal traffic); see also, Order, EB-TCD-26-00041364, DA 26-873, released August 27, 2026 (notifying nine companies of

proceedings are costly, damage reputations, and could ultimately result in removal from the RMD – effectively putting a company out of business. Any suggestion that the vast majority of VSPs ignore these risks is not supported by the record in this or any other proceeding. To the contrary, the data suggests that most upstream VSPs and end user customers are adequately vetted, and in those rare circumstances if illegal calling is suspected, VSPs are proactively suspending or terminating those callers. This explains why such a small number of VSPs are responsible for most of the illegal calls

B. The Commission should not deputize the STI-GA or any other third party to determine whether a VSP should be permitted to offer regulated communications services.

An SPC token is a credential for participation in the STIR/SHAKEN ecosystem, not a federal license to provide voice services. Numeracle proposes to transform the token from a standards-based technical trust credential into market access authorization. VON correctly explained that STIR/SHAKEN identifies the provider that signed or originated a call so that the FCC, state attorneys general, the ITG, and other authorized bodies can identify the responsible provider and take appropriate action. The STI-GA was not created to decide who may provide voice service in the United States.

Importantly, the STI-GA also explains that STIR/SHAKEN provides cryptographic identification supporting traceback and enforcement. It was not designed as a comprehensive caller-identity system or a licensing structure. Moreover, STI-GA explained that it is not staffed, funded, or legally structured to act as a federal enforcement body. There is broad agreement among commenters that this is the case.

---

deficiencies in their Robocall Mitigation Database certifications related to a failure to respond to traceback requests from the industry traceback consortium).

There is broad agreement that the Commission alone is the designated gatekeeper for regulatory compliance and can do so through the RMD and other enforcement tools. The Commission should not convert private verification vendors or industry governance bodies into de facto regulators. Efforts are best focused on strengthening and building upon technology-neutral standards which will enable a more accurate and enforceable RMD allowing for flexibility in KYC and KYUP practices through safe-harbors that are risk-based and further reinforce the necessary completion of an all-IP transition.[8]

C. The Commission should permit all initiating providers to sign calls

VON also recommended against limiting STIR/SHAKEN signing authority to originating service providers ("OSPs") alone. Any initiating provider capable of signing its own calls should be permitted, and encouraged, to obtain its own SPC token and sign its own calls directly, rather than being forced to route calls through specific upstream facilities-based providers.[9] The initiating provider is best positioned to authenticate traffic because it assigns the phone numbers, monitors calling patterns and has commercial incentives to prevent fraudulent use of its service. Requiring it to hold its own SPC token also means it goes through the same vetting the STI-GA applies to every other token holder and ensures that the actual SPC token holder maintains direct

---

[8] Other comments similarly recommend flexible KYUP practices that can adapt to market changes and emerging threats. See, e.g., Comments of T-Mobile USA, Inc., CG Docket No. 17-59, at 4-6 (filed August 10, 2026); Comments of CTIA, CG Docket No. 17-59, at 9-15 (filed August 10, 2026); Joint Comments of Incompas and the Cloud Communications Alliance, CG Docket No. 17-59, at 12-14 (filed August 10, 2026).

[9] "Initiation" is the action performed by a voice service customer in commencing a call; it does not include origination. "Initiating provider" is a VSP that performs initiation for its end users' calls (i.e., a non-facilities-based provider serving end users directly). In the case of a UCaaS provider, the call initiates on the UCaaS provider's point of presence; the UCaaS provider puts in the SIP header and the information necessary to send the call to the called party, including STIR/SHAKEN information and signs the call before passing it to the wholesale carrier, who puts the call on the PSTN and delivers it to the called party's terminating carrier.

responsibility and accountability for illegal traffic. This also keeps the call transparent. Today, when an initiating provider signs a call, the terminating provider can see who the initiating provider is. That visibility would disappear if only originating providers could sign calls, especially since delegated certificates are not yet widely adopted, and in most cases not meaningfully offered at all. The Commission should therefore allow both initiating and originating providers to sign calls.

Adoption of VON's proposal would alleviate the liability concerns raised by CTIA and T-Mobile if initiating providers make the attestation decision but facilities-based providers sign the calls. CTIA recommends that responsibility follow the decision-maker: "the provider responsible for making the attestation — the initiating provider — would also be responsible for improper attestations."[10] If the initiating provider signs its own calls, it *is* the SPC token holder — responsibility follows the signature automatically, no new liability rule needed.

This approach is preferable to trying to expand the definitions of "originating provider" and "facilities-based" to encompass all entities with call signing ability. Many, if not most, initiating providers, do not have physical facilities and are not "facilities-based" by the plain meaning of the words. Trying to expand the definition beyond a common-sense meaning is unnecessary to achieve all commenters' goals of being able to retain their existing signing authority.

---

[10] Comments of CTIA at 19-20. T-Mobile suggests a good-faith-reliance safe harbor for OSPs who sign based on someone else's attestation decision. Comments of T-Mobile at 12-13. Under VON's proposal, OSPs are never asked to sign based on another provider's decision, obviating the need for the safe harbor.

CONCLUSION

VON urges the Commission to provide VSPs with the flexibility needed to vet upstream providers and make decisions consistent with their business models on how best to ensure they are not responsible for originating or transporting illegal calls.

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

September 8, 2026