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
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
Dismissal of Outdated or Otherwise Moot Robocall Petitions	)	CG Docket No. 25-307

COMMENTS OF THE VOICE ON THE NET COALITION

The Voice on the Net ("VON") Coalition[1] hereby submits these comments in response tothe Ninth Further Notice of Proposed Rulemaking in CG Docket No. 17-59; Seventh Further Notice of Proposed Rulemaking in WC Docket No. 17-97; Further Notice of Proposed Rulemaking in CG Docket No. 02-278; Public Notice in CG Docket No. 25-307 (the "*FNPRM*")[2] in the above-referenced dockets. VON strongly supports the Commission's efforts to reduce illegal and spoofed robocalls and to move the industry towards wide-spread adoption of Rich Call Data ("RCD"). VON submits these comments to highlight how the STIR/SHAKEN framework and RCD can work hand in hand to reduce illegal calls and to request that the

[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] Ninth Further Notice of Proposed Rulemaking in CG Docket No. 17-59; Seventh Further Notice of Proposed Rulemaking in WC Docket No. 17-97; Further Notice of Proposed Rulemaking in CG Docket No. 02-278; Public Notice in CG Docket No. 25-307 (rel. October 29, 2025); see also, 90 Fed. Reg. 56101 (Dec. 5, 2025)(establishing a comment date of January 5, 2026).

Commission ensure any rules are competitively neutral and do not stifle innovation or harm U.S. businesses and consumers.

DISCUSSION

The Need for all IP Networks. As the Commission recognizes in the ongoing IP-to-IP interconnection proceeding, [3] all-IP networks are a prerequisite for restoring trust in the voice ecosystem and supporting the STIR/SHAKEN caller ID authentication framework. Non-IP technology at any point in the call path creates gaps that can be exploited by bad actors and limits the efficacy of STIR/SHAKEN.[4] As others have noted, a significant percentage of calls still arrive at terminating providers without authentication because the STIR/SHAKEN headers are stripped whenever the call hits TDM in the call path. The same would be true for any RCD or other caller name information placed within a SIP header. Thus, all-IP networks are also necessary for full implementation of STIR/SHAKEN and to support branded calling/RCD and other future capabilities that can work together to restore trust in calling. As the Commission notes, "Completing the IP transition thus remains the surest path to ensuring that consumers and businesses can take full advantage of the tremendous benefits, efficiencies, and increased reliability and security of next-generation networks."[5] The Commission must ensure that caller ID authentication is carried from origination to termination and ensure that the IP transition is complete before imposing additional obligations on voice service providers ("VSPs") to build RCD capabilities into existing networks.

[3] *Notice of Proposed Rulemaking,* WC Docket No. 25-304, WC Docket No. 25-208, WC Docket No. 17-97 (rel. October 29, 2025) (hereinafter "*IP Transition NPRM*").
[4] *IP Transition NPRM* at para. 14.
[5] Id.

The Role of STIR/SHAKEN. In the FNPRM, the Commission asks whether transmitting caller identity verification should be a condition of A-level attestation.[6] VON recommends against adopting any rule that would conflate the purposes of STIR/SHAKEN and caller name verification. STIR/SHAKEN was designed as a network-level tool that would allow service providers to pass information about whether the caller identification is valid. The STIR/SHAKEN purpose and framework has criteria for US VSPs to (i) be a trusted provider in order to obtain a token, (ii) sign calls with their token under a protocol based in non-proprietary standards; (iii) under an accepted criteria, using an attestation of either A,B, or C, to represent that the provider knows the telephone number and whether the caller has a right to use the telephone number, and importantly, (iv) facilitate tracebacks. STIR/SHAKEN is not intended to judge the intent of the caller or to assure the called party that the caller is calling for legitimate purposes. Instead, it was meant to assure the terminating *provider*, at the network level, that the caller has the right to use the phone number. That is why most terminating providers do not inform their customers what attestation level the call was given. At most, some terminating providers rely on this information to decide whether to block or generically label the call.

Requiring providers to pass along caller name information if they sign a call with an A attestation could effectively eliminate legitimate A-level attestations in many scenarios, reducing the usefulness of STIR/SHAKEN for analytics and consumer trust, without protecting consumers.[7] Instead, the Commission should use RCD as a way build upon the existing STIR/SHAKEN framework and provide crucial information directly to called parties.

[6] *FNPRM* at para. 65.
[7] Id. at para. 68.

Rich Call Data (RCD). As discussed in the *FNPRM*, RCD builds upon the STIR/SHAKEN framework by increasing the amount of data the originating VSP can transmit with a call over an IP network using encryption.[8] Under the RCD standards, and subject to capacity limits, this data may include caller identity information such as name, photo, logo, email address, location, and the reason for the call.[9] RCD is implemented through standards developed by two industry groups, the Alliance for Telecommunications industry Solutions (ATIS) and the Internet Engineering Task Force (IETF).[10]

VON supports the Commission's proposal to require all VSPs to be able to accept RCD and transmit the information directly to called parties. RCD should be made available under protocols based on non-proprietary standards that are honored across the network regardless of the provider and will allow all VSPs to accept RCD. Like STIR/SHAKEN, customer verification could be managed by trusted, neutral third parties. If these third parties attest that that they have verified the calling party, terminating carriers should be required to accept and display RCD. Terminating carriers should not get to choose from which upstream providers they will accept RCD or require upstream providers to transmit RCD only through a carrier's chosen partner. VON notes that any RCD requirement should become effective only after the IP-to-IP interconnection is complete to ensure that VSPs can first focus on transitioning to all IP networks.

As the leader in the development and implementation of STIR/SHAKEN, the United States should encourage the adoption of open standard RCD built on STIR/SHAKEN so that it can be used globally providing a benefit to US providers and callers. Efforts are underway to

[8] Id. at para. 12.
[9] Id.
[10] Id.

facilitate cross border call authentication using STIR/SHAKEN over an international transit network, using both US and international numbers.[11] The organization spearheading this effort is in the process of obtaining approval from STI-GA to interoperate with the US STIR/SHAKEN system. If approved, there will be a vetting system for legitimacy and enforcement procedures at the network level including traceability. It will also benefit RCD, which can be used to transmit the caller's identity when the originating VSP wants to share it with the terminating providers.

Marking international calls. VON recommends against restricting NANPA phone numbers from being assigned to US customers' agents located overseas. Many U.S. corporations rely on foreign call centers to provide low-cost round the clock support to their customers. Preventing corporations form assigning NANPA phone numbers to these agents would harm American consumers and increase consumer cost without preventing illegal calls. VON also recommends against requiring "gateway providers to mark calls that originate from outside of the United States, intermediate providers to transmit that information to downstream providers, and the terminating voice service provider to transmit to consumers' handsets an indicator that a call originated outside of the United States when they know or have reason to know that a call originated from outside of the United States, such as when a call has been marked as having originated outside of the United States by an gateway provider."[12]

There is a significant amount of traffic that comes into the United States from

[11] See, e.g., ATIS Cross Border Call Authentication Trial Results Report, found at: https://cdn.atis.org/atis.org/2025/01/17180008/CBCA-Trial-Report-vFinal.pdf#:~:text=The%20CBCA%20tests%20outlined%20in,deployment%20of%20STIR%2FSHAKEN%20for%20all (last visited December 31, 2025).
[12] Id. at para. 70.

international locations, gateway solutions that mark traffic as internationally originated should not undermine user receipt of legitimate calls. Legitimate international traffic should not be disproportionately blocked. This is especially a concern when analytics services are used, or it results in a new payment scheme that assesses a fee on service providers to verify their traffic as legitimate prior to a gateway provider routing that traffic to its final destination.

There are legitimate uses, notably call centers, inbound to the United States and outbound from the United States to other international markets as a reason to not identify a call as foreign originated.[13] Accordingly, VON supports an exemption from any requirement to mark international traffic for calls that originate on devices subscribed to United States VoIP services and that are roaming or operating outside the United States.[14] For example, as the Commission notes, VoIP consumers may seek to use nomadic capabilities of their service to place calls using their United States telephone number while traveling or working abroad.

Instead, the Commission should leverage STIR/SHAKEN and industry developed processes, such as the Cross Border Call Authentication framework. The CBCA relies on STIR/SHAKEN to verify that calls entering the U.S. through international gateways are authorized to use U.S. phone numbers. The Commission should encourage other countries to adopt the U.S.'s STIR/SHAKEN framework so they can leverage the CBCA to verify that calls traversing international gateways are authorized to use domestic phone numbers and should be passed along to terminating providers.

[13] Because of the proliferation of call centers based outside the United States serving US companies, the Commission should not prohibit call spoofing of US numbers that originate outside of the United States. See, Id. at para. 86.
[14] Id. at para. 75.

Definition of Caller Identity Information. The FCC proposes to define "caller identity information" as having the same meaning given the term "caller identification information" in 47 § CFR 64.1600(c) of its rules, but exclude the originating telephone number, portion of a telephone number and billing number information, per the definition of "information regarding the origination" in 47 § CFR 64.1600(g)(1)(2) and (5).[15] This would then require the inclusion of name, location information and other information regarding the source or apparent source of a telephone call.

There is not a one-size fits all approach. The Commission should not adopt prescriptive measures, limit flexibility, or proprietary solutions. Doing so could harm competition and make the United States an outlier. There are numerous reasons businesses may want flexibility in the definition of caller identity information. This may include situations where the customer of record may not be the actual caller or the caller may sit behind a common number, for example, Walmart, Delta, and Microsoft. A doctor's office or a ridesharing or food delivery service may not want to expose the actual telephone number of the doctor, driver, or customer, in order to maintain the privacy of the calling and called parties. Moreover, for nomadic VoIP providers, whose end users can access the service from multiple devices (including mobile devices) and any broadband connection, defining and requiring location information can be difficult, if even feasible. Thus, location should be optional, and not a required dataset.

[15] Id. at para. 27.

CONCLUSION

The Commission should act in accordance with the recommendations herein

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

January 5, 2026