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

In the Matter of	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these comments in response to the Sixth Further Notice of Proposed Rulemaking ("*Sixth Further Notice*") [2] adopted by the Federal Communications Commission ("Commission") in the above-captioned proceeding. The *Sixth Further Notice* seeks comment on, among other things, third-party caller-ID authentication arrangements that exist between service providers and the entities that perform authentication on their behalf.[3] While these services are a valuable option for providers' compliance with the Commission's caller-ID authentication rules, the potential for bad actors to utilize certain variations of these arrangements in a way that could undermine the integrity of the STIR/SHAKEN ecosystem cannot be overlooked. Safeguards as proposed herein are necessary to maintain trust in the STIR/SHAKEN ecosystem and allow these arrangements to function as intended for legitimate providers.

A recently filed TransNexus *ex parte* letter[4] highlights the problematic nature of a *subset* of these third-party authentication arrangements (specifically "third-party signing" as

[1] NTCA–The Rural Broadband Association represents approximately 850 independent, community-based companies and cooperatives that provide advanced communications services in rural America and more than 400 other firms that support or are themselves engaged in the provision of such services.
[2] *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) ("*Sixth Report and Order*" or "*Sixth Further Notice*").
[3] *Id*., ¶¶ 97-107.
[4] TransNexus *ex parte* letter, WC Docket No. 17-97 (fil. May 22, 2023) ("TransNexus *ex parte*").

TransNexus rightly labels it).[5] Under these arrangements, the third-party entity performs the authentication process using its own certificate to "sign" calls on behalf of originating service providers ("OSPs"). The OSPs utilizing third-party signing are neither registered with the Secure Telephone Identity Policy Authority ("STI-PA") nor registered with a STI Certificate Authority ("STI-CA"), meaning they obtain neither the tokens nor the certificates that are critical to reliable call authentication. As TransNexus discusses in detail, this scenario runs counter to the STIR/SHAKEN standards.[6]

Putting aside technical standards, these third-party signing arrangements pose substantial risk of undermining the integrity of the STIR/SHAKEN ecosystem, even if in most cases they are not intended for nefarious use. As a threshold matter, the terminating provider cannot reliably identify the OSP that is the first provider in a call chain when a call is authenticated under these "third-party signing" arrangements – which is perhaps the most fundamental of concepts to meaningful and reliable call authentication. One of the virtues of providers' use of STIR/SHAKEN is to identify to the OSP – "traceback" efforts that get to the source of illegally spoofed calls are bolstered by every operator in a call chain passing STIR/SHAKEN identity headers end-to-end. Yet the use of these third-party signing services masks the identity of the OSP, and it is not difficult to envision how bad actors (OSPs and the third parties "signing" on their behalf) might exploit such arrangements. Simply put, when third-party signing arrangements are employed, the terminating provider has far less ability to distinguish between an illegally spoofed call and a legitimate call that complies with all of the Commission's caller-

[5] *Id*., p. 1 ("We distinguish this arrangement, which we refer to as "third-party signing," from a scenario where an OSP uses an external "signing service." A signing service performs call authentication by creating a signature using the OSP's STI certificate and with an attestation level that the OSP provides in conformance with the ATIS STIR/SHAKEN standards and the OSP's knowledge of the call initiator and calling number.").
[6] *See Id*., pp. 3-4.

ID/STIR/SHAKEN rules. As TransNexus notes, "bad actors, including persons that initiate illegal robocalls and the OSPs that originate such robocalls, are enabled to hide illegal robocalls amidst other calls authenticated by the third party."[7]

In addition, the continued use of these arrangements could undermine the value of STIR/SHAKEN for legitimate providers. If blocking tools that employ data analytics cannot easily distinguish between legitimate and illegally spoofed calls – because "bad actors…are enabled to hide illegal robocalls amidst other calls authenticated by the third party"[8] – the possibility arises that voice service providers' legitimate and authenticated calls that are conveyed consistent with the STIR/SHAKEN standards could be mislabeled. Consumers using a legitimate "good actor" provider, that has itself expended substantial resources to authenticate calls in a way the standard was meant to be used, deserve better than to have their legitimate calls labeled as "spam" simply because they have been essentially commingled with questionable OSP calls leveraging third-party signing capabilities.

Fortunately, closing this vulnerability in the STIR/SHAKEN ecosystem is relatively simple. The Commission merely needs to require that all OSPs using "third-party signing" arrangements themselves register with the STI-PA and a STI-CA to procure their own tokens and certificates, and that their own certificates are then used to sign each originating call. While NTCA is certainly sympathetic to concerns regarding cost given its representation of smaller operators, these requirements are simple and relatively inexpensive – and the low cost of obtaining tokens and certificates is certainly outweighed by the benefit of closing a serious

[7] *Id*., p. 2.
[8] *Id*.

security vulnerability that could harm consumers and undermine the industry's extensive investment in STIR/SHAKEN.

To be clear, NTCA does not support a prohibition or even limits[9] on the use of third-party authentication services of any kind. Rather, the question presented here is simply one of whether "third-party signing" services specifically as described above could be leveraged to undermine the integrity of the STIR/SHAKEN ecosystem. The Commission has made clear its commitment to combatting illegal robocalls/spoofed calls that plague and victimize consumers, and as part of its efforts to protect consumers has sought to identify and close vulnerabilities in the system at every turn.[10] Here, a vulnerability has been identified, and a simple solution is readily available to close it and safeguard the STIR/SHAKEN ecosystem.

By: /s/ Michael R. Romano
Michael R. Romano
Executive Vice President
mromano@ntca.org

By: /s/ Brian J. Ford
Brian J. Ford
Vice President – Federal Regulatory
bford@ntca.org

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203

June 5, 2023

[9] *Sixth Further Notice*, ¶ 97.
[10] *See Sixth Report and Order*, ¶¶ 7-10.