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 USTELECOM – THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association ("USTelecom")[1] submits these reply comments in response to the Federal Communications Commission's ("Commission's") Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 ("*Further Notice*") proposing new requirements to address foreign-originated illegal robocalls.[2]

The record demonstrates that additional Commission action is necessary to stop the onslaught of foreign-originated robocalls. Many commenters also agree that any new rules should apply to all providers – and not just gateway providers – to ensure a clear, consistent, and streamlined approach. The Commission's ultimate goal should be to establish a chain of trust for

[1] USTelecom is the premier trade association representing service providers and suppliers for the communications industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks. Its diverse membership ranges from international publicly traded corporations to local and regional companies and cooperatives, serving consumers and businesses in every corner of the country. USTelecom leads the Industry Traceback Group ("ITG"), a collaborative effort of companies across the wireline, wireless, VoIP and cable industries actively working to trace and identify the source of illegal robocalls. The ITG was first designated by the Commission as the official U.S. robocall traceback consortium in July 2020.

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105 (rel. Oct. 1, 2021) ("*Further Notice*").

voice traffic destined to the United States. A complete chain of trust will best enable the Commission and industry to take action to stop illegal traffic. In contrast, new gateway-specific requirements, including new blocking mandates, will be ignored by fly-by-night bad actor service providers, create unintended consequences, and leave gaps in the regime while placing additional burdens on providers who already protect the network from these calls.

Finally, the record does not support requiring gateway providers (or any other immediate providers) to sign unauthenticated traffic, which would be exorbitantly costly for some providers without providing commensurate anti-robocalling benefits.

I. THE RECORD SUPPORTS ENHANCING AND LEVERAGING THE COMMISSION'S EXISTING REGIME

A. The Commission Should Require that All Providers Submit Certifications in the Robocall Mitigation Database and Implement a Robocall Mitigation Program

Most commenters agree that the Commission should look to enhance its existing regime, rather than infuse additional complexity through gateway provider-specific rules.[3] Put simply, "[v]oice service providers should not have one set of obligations when acting as a voice service provider and another while acting as a gateway provider."[4] To that end, "[w]hile imposing existing obligations more broadly throughout the calling ecosystem would benefit called parties and voice service providers … gateway providers should not be obligated to comply with additional redundant and unnecessary mitigation requirements."[5] Instead, "gateway providers

[3] *See, e.g.,* CTIA Comments at 8; INCOMPAS Comments at 7; T-Mobile Comments at 5; Twilio Comments at 3; ZipDX Comments at 32.

[4] T-Mobile Comments at 6.

[5] *Id.* at 5.

should generally be subject to the same obligations as other voice service providers and intermediate providers (as appropriate)."[6]

USTelecom agrees. The Commission can best avoid infusing additional, unneeded complexity by enhancing and leveraging its existing regime. In particular, the Commission should close the intermediate provider loophole, requiring that all voice service providers implement a robocall mitigation program and certify to such in the Robocall Mitigation Database ("RMD"). There is ample support in the record for closing the intermediate provider loophole, as well as for requiring that all providers implement a robocall mitigation program. Twilio, for instance, suggests that "[r]equiring all intermediate providers to submit certifications to the RMD will ensure that the Commission and industry alike have full visibility into the universe of providers that are responsible for fighting illegal robocalls and allow parties to evaluate the sufficiency of the robocall mitigation plans that each of those providers has described."[7] In addition to ensuring transparency, it also will encourage accountability. As CTIA notes, "[p]romoting robocall mitigation by intermediate providers will promote use of [robocall mitigation] techniques by all entities in the call path and in turn help protect U.S. networks from illegal traffic."[8]

USTelecom has consistently advocated that the Commission should require providers to implement a robocall mitigation program regardless of whether they have implemented

---

[6] Twilio Comments at 3.

[7] *Id.*; *see also, e.g.*, iBASIS Comments at 13 ("As an intermediate provider, iBASIS is already in the database, but has no current obligation to submit a robocall mitigation plan. iBASIS believes that it is appropriate to require such a submission."); Comcast Comments at 10 (supporting requiring gateway providers to submit a certification to the RMD to give the FCC and other service providers broader visibility).

[8] CTIA Comments at 7.

STIR/SHAKEN.[9] A robocall mitigation program can help to ensure that providers take proactive steps to prevent illegal robocalls, including those made by scammers using blocks of seemingly legitimately-assigned numbers, whereas STIR/SHAKEN alone cannot address that issue. The Commission should now extend the robocall mitigation program requirement to all providers in all contexts.

For an intermediate provider's robocall mitigation efforts as part of any such program, the record supports the proposition that providers undertake at least a basic level of vetting of the providers from whom they directly accept traffic. As CTIA explains, "[p]roviders, including intermediate and gateway providers, already implement robust [know-your-customer] for their interconnection partners."[10] Twilio notes further that such due diligence helps to "ensure that the upstream providers that deliver traffic to them are legitimate, authorized service providers."[11] With proper vetting for foreign-originated traffic in particular, providers can "take concrete steps to obtain information about … foreign carriers before carrying their traffic into the United States."[12] Vetting of interconnection partners should be part of every provider's robocall mitigation program.[13]

[9] *See, e.g.*, USTelecom Comments at 6; Comments of USTelecom – The Broadband Association, WC Docket No. 13-97, WC Docket No. 07-243, WC Docket No. 20-67, IB Docket No. 16-155, at 2, 5-6 (filed Oct. 14, 2021).

[10] CTIA Comments at 12-13.

[11] Twilio Comments at 4.

[12] Comcast Comments at 9. The record, however, makes explicitly clear that intermediate providers, including acting as gateway providers, can only vet their upstream provider, and have no realistic way to vet the caller. *See, e.g.*, USTelecom Comments at 5 n.6; Comcast Comments at 9-10; i3Forum Comments at 9; iBASIS Comments at 12-13; T-Mobile Comments at 7-8; Twilio Comments at 3-4.

[13] *See also* USTelecom Comments at 4-5 (stating that providers also should include in a robocall mitigation program the process and actions they take when they are notified by other providers, the Commission, or the traceback consortium regarding illegal traffic on their network).

By closing the intermediate provider loophole and requiring that all providers submit certifications in the RMD and implement robocall mitigation programs, the Commission will take a step towards realizing a chain of trust through which all U.S.-destined traffic that utilizes U.S. numbers – whether originating domestically or abroad – flows exclusively. In particular, it will allow the Commission to take direct action should a provider break the chain of trust and accept traffic from an intermediate provider that is not in the RMD. It also will complement existing industry efforts, including traceback, and allow the industry to build out new tools and mechanisms, including with regard to provider vetting, that can further enhance accountability along the call path.

B. Mandatory, Prescriptive Mitigation Requirements Will Create Unintended Consequences

Commenters in the record identify significant concerns about the Commission's proposals to mandate blocking at the gateway, including on a per-call basis. As one commenter explains, "[b]locking calls is a serious and complicated action that must be precisely and judiciously applied to avoid blocking lawful traffic."[14] In addition, "blocking foreign-originated calls requires global synchronization among all service providers that have a role in transmitting a call," a task that is "difficult, if not impossible…."[15] Moreover, "[b]locking in all instances may not be the most effective strategy in addressing identified illegal traffic[.]"[16] To be clear, blocking is a powerful and critical tool in a provider's anti-robocalling arsenal, and the

[14] i3forum Comments at 6.

[15] *Id.* The Commission's ongoing proceeding regarding the best method to inform call originators that their calls have been blocked underscores the challenges involved. *See generally Advanced Methods to Target and Eliminate Unlawful Robocalls – Petition for Reconsideration and Request for Clarification of USTelecom – The Broadband Association*, Order on Reconsideration, Sixth Further Notice of Proposed Rulemaking, and Waiver Order, CG Docket No. 17-59, FCC 21-126 (rel. Dec. 14, 2021).

[16] iBASIS Comments at 9

Commission therefore should ensure that all providers feel empowered to block the calls for which they have a reasonable basis to believe are illegal.[17] But an inflexible blocking mandate puts legitimate calls at risk, in addition to causing implementation challenges and creating the potential for unintended consequences.[18]

There also is no reason for, and potential unintended consequences from, mandating that providers monitor and treat types of traffic differently, as one commenter suggests.[19] Mandating such a prescriptive approach could impose substantial burdens on those voice service provides already leading the fight against illegal robocalls, while doing little to address the behavior of those intentionally ignoring the rules and seeking to evade accountability altogether. It also would introduce more complexity into the Commission's already-complicated anti-robocall legal regime. That said, for many providers, monitoring for and treating distinct types of traffic differently may be an essential part of those providers' robocall mitigation programs. But it should not and need not be a prescriptive mandate.

The Commission can better achieve the underlying goal associated with the blocking and monitoring proposals by requiring that all providers implement a robocall mitigation program and maintaining the agency's existing permissive call-blocking framework.[20]

---

[17] *Cf.* Comcast Comments at 8-9 (Commission should adopt a clear and broad safe harbor for any blocking requirements); TNS Comments at 3 (Commission should provide gateway providers with a blocking safe harbor).

[18] Given the problems that can flow from rigid, mandatory blocking requirements, the Commission should take this opportunity to restate that providers are encouraged, but not legally required, to block calls, whether they are from invalid, unallocated, or unassigned numbers or numbers on an industry Do Not Originate list, or based on reasonable analytics. *Cf.* INCOMPAS Comments at 12 (discussing case against intermediate carriers in a call path). Indeed, indiscriminately blocking all calls from invalid, unallocated, or unassigned numbers can result in the blocking of legitimate calls, including some critical ones. *See* USTelecom Comments at 12.

[19] *See* ZipDX Comments at 26-27, 29, 37.

[20] *See, e.g.*, CTIA Comments at 12.

II. THE RECORD DOES NOT SUPPORT A REQUIREMENT THAT GATEWAY PROVIDERS SIGN UNAUTHENTICATED CALLS

The record does not support the Commission's proposal to require that gateway providers sign unauthenticated calls.[21] Commenters note that because gateway providers in most cases will not know the provider that originated the traffic, gateway providers generally only would be able to provide a C-level attestation to such calls.[22] Such attestation would provide almost no benefit at an extensive and disproportionate cost, particularly for large facilities-based providers that atypically are conduits for unlawful traffic into the United States.

The commenters that support a new gateway provider STIR/SHAKEN requirement cite faster traceback and improved call analytics, as well as the potential of eliminating the foreign provider prohibition (*i.e.*, limiting any chain of trust to only U.S. entities).[23] None of these commenters address the substantial costs that some providers would have to undertake to sign traffic at the gateway nor whether such costs would be commensurate with the purported benefits. Indeed, any benefits would *not* be commensurate with the costs. As USTelecom noted in initial comments, the industry traceback process has become so quick and efficient that C-level attestations offer at best a marginal benefit for traceback.[24] In addition, it's not clear that a proliferation of C-level attestations would provide additional useful information for call analytics.[25] Indeed, C-level attestations only indicate the provider did not know whether or not

[21] *See, e.g.*, USTelecom Comments at 9-11; AB Handshake Corporation Comments at 4; CTIA Comments at 14; i3forum Comments at 3-4; iBASIS Comments at 5; iconectiv Comments at 3.

[22] *See* USTelecom Comments at 9-10; AB Handshake Corporation Comments at 4; i3forum Comments at 5; iBASIS Comments at 5; *see also* Comcast Comments at 6.

[23] *See* Comcast Comments at 5-6; INCOMPAS Comments at 7-8; T-Mobile Comments at 3.

[24] USTelecom Comments at 11.

[25] *See, e.g.*, i3forum Comments at 5 (C-level attestation "fails to provide any useful or meaningful assistance for blocking illegal robocalls").

the originator is authorized to use the number and that the call was signed by a gateway. That information may already be obvious without such attestation and therefore is of limited value. Moreover, gateway provider attestations would not replace the benefits of a full chain of trust that includes all providers – foreign and domestic – that are in the call path of traffic from U.S. numbers terminating to U.S. numbers. Seeking to establish a full call path chain of trust is the better public policy approach.

That's not to say gateway providers (or other intermediate providers) never should sign unauthenticated traffic. Consistent with relevant standards, gateway providers should feel free to work with upstream partners to sign traffic as A, B, or C as appropriate.[26] But the Commission should not adopt a gateway provider authentication mandate, and doing so would fail any reasonable cost-benefit analysis.[27]

There also is no reason to change the Secure Telephone Identity Governance Authority's ("STI-GA's") token access policy.[28] In particular, should the Commission eliminate the intermediate provider loophole and require all providers to file a certification in the RMD, gateway providers should be able to get a token in most if not all contexts. Specifically, any provider that transits traffic as part of its business should have a Form 499-A on file with the Commission; any gateway provider should have, or can obtain, an Operating Company Number (OCN), and, with the new requirement proposed by USTelecom, every gateway provider will

[26] *See* iconectiv Comments at 2.

[27] *See* USTelecom Comments at 11*; see also* i3forum Comments at 5 ("It would be wasteful and unfair to require gateway providers to invest their resources in attempting to comply with STIR/SHAKEN when the outcome does not facilitate the identification or elimination of illegal robocalls.").

[28] *See Further Notice* ¶ 47.

have submitted certifications in the RMD.[29] To the extent that there are providers that do not meet these conditions but still desire access to a token, changing or waiving the requirements risks creating a new loophole through which bad actor providers can more easily obtain tokens without sufficient oversight and accountability. The Commission should work in this and other anti-robocall proceedings to eliminate existing potential loopholes, and should not create new ones.

III. CONCLUSION

The record includes clear endorsement of additional Commission action to address foreign-originated illegal robocalls. It, however, does not support new requirements focused exclusively on gateway providers, nor new prescriptive blocking and burdensome authentication mandates. Instead, the Commission should work to refine and enhance its existing RMD regime, including by ensuring that all providers in the call path have robocall mitigation programs and submit certifications in the RMD. Doing so will help to ensure a full chain of trust in the call path of calls destined to the U.S. subscribers. It also will aid accountability if and when that chain is broken.

[29] *See id.* (noting that the STI-GA's token access policy requires entities to have 1) a current FCC Form 499-A; 2) an OCN; and 3) direct access to numbering resources or an RMD certification). Separately, one commenter, TransNexus, suggests that the Commission should begin the process to phase out the non-IP extension. TransNexus Comments at 1-2. There is an active and ongoing conversation in the industry regarding long term solutions to address the IP interconnection challenge. In the meantime, providers should not be forced to use particular vendors and implement short-term, potentially inferior solutions. Nor would it be appropriate for the Commission to address the non-IP extension here, as it is not directly germane to addressing foreign-originated robocalls.

Respectfully submitted,

By: */s Joshua M. Bercu /*

Joshua M. Bercu
Vice President, Policy & Advocacy

USTelecom – The Broadband Association
601 New Jersey Avenue, N.W.
Suite 600
Washington, D.C. 20001
(202) 551-0761

January 10, 2022