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

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor	)	CG Docket No. 17-59
	)	
	)	
	)	

COMMENTS OF
USTELECOM – THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association ("USTelecom")[1] submits these comments in response to the Fourth Further Notice of Proposed Rulemaking ("*Fourth FNPRM*") in the above-referenced docket.[2]

I. INTRODUCTION AND SUMMARY

In July, the Commission took an important step to implement several of Congress' mandates in the TRACED Act and to further the efforts of voice service providers and their partners to protect consumers from illegal robocalls. Specifically, by adopting a safe harbor for blocking calls based on reasonable analytics, as well as adopting a safe harbor for blocking calls from bad-actor providers, the Commission further empowered voice service providers to stop robocalls before they get to consumers.[3] Although the Commission did not include network-

[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 also 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 designated by the FCC 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, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, CG Docket No. 17-59, FCC 20-96 (rel. July 17, 2020) ("*Third R&O*" when referring to the Third Report and Order and "*Fourth FNPRM*" when referring to the Fourth Further Notice of Proposed Rulemaking).

[3] *Third R&O* ¶ 21.

level call blocking in the safe harbors,[4] the Commission recognized the importance of blocking calls in the network that are highly likely to be illegal and proposed to adopt a safe harbor for such blocking in the accompanying *Fourth FNPRM*, a proposal that USTelecom strongly supports.[5] The Commission also appropriately recognized that additional work remains to protect consumers, including by further implementing aspects of the TRACED Act.[6]

As the Commission moves forward, it should be guided by its ultimate goal: to stop illegal and unwanted robocalls. The Commission can best do so by empowering service providers to take the steps necessary to prevent such calls from reaching their destination. Doing so is not just good for consumers – it also directly benefits calling parties whose calls will go unanswered if consumers lack trust in the telephone network. By the same token, USTelecom appreciates the importance of ensuring that legal calls that consumers want to receive are not inappropriately blocked or mislabeled. After all, to ensure trust in the telephone network, voice service providers must deliver the calls that their customers desire and expect, which necessitates clear and sufficient processes to address any claims of inappropriate blocking or labeling. The Commission has endorsed an industry-led, flexible approach in the STIR/SHAKEN and traceback contexts, rather than prescriptive regulations, and should maintain that approach on these issues as well.

The Commission therefore should look for ways that enhance the efforts of industry leaders, while ensuring that the industry continues to have the flexibility needed in this unremitting fight against robocalls. To that end, the Commission should, as the *Fourth FNPRM* proposes, impose certain additional obligations on voice service providers that will ensure that

[4] *Id.* ¶ 49.

[5] *Fourth FNPRM* ¶ 104.

[6] *See, e.g., id.* ¶¶ 88-90.

all voice service providers – rather than just industry leaders like the companies that comprise the Industry Traceback Group ("ITG") – do their part to stop robocalls. Specifically, the Commission should require all voice service providers to respond to traceback requests and should impose affirmative robocall mitigation obligations on voice service providers when they originate robocalls. The Commission also should continue to afford service providers flexibility to empower them to protect their customers from illegal robocalls, including by extending the safe harbor for reasonable analytics to network-level blocking and encouraging calling parties and voice service providers to work together to develop industry best practices for mitigating mislabeling or over-blocking, rather than adopting prescriptive regulations.

II. ADDITIONAL COMMISSION ACTIONS ARE NECESSARY TO IMPEDE THE FLOW OF ILLEGAL ROBOCALLS

A. Voice Service Providers Should Be Required to Respond to Traceback Requests

The Commission should require all voice service providers to respond to traceback requests, whether such requests come from the Commission, law enforcement, or the ITG as the designated Traceback Consortium.[7]

The traceback process developed and run by the ITG is already a resounding success. In 2019, the ITG conducted over 1,000 tracebacks with participation from more than 100 companies, implicating more than 10 million illegal robocalls and leading to more than 20 subpoenas and/or civil investigative demands.[8] This year, the ITG has already surpassed those 2019 marks, and has seen significant growth in industry interest, membership, and cooperation.

---

[7] *See Fourth FNPRM* ¶ 96; *see also Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, DA 20-785 ¶ 28 (EB rel. July 27, 2020) ("*Traceback Consortium Order*").

[8] *See generally* USTelecom Industry Traceback Group, *2019 Progress Report* (2019), https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg/.

Perhaps more important, voice service providers and state and federal law enforcement agencies increasingly rely on traceback results to cut off the flow from illegal callers in the first instance.

Nevertheless, although trending down in response to enforcement agencies' validation of the traceback process, the ITG's tracebacks at times still do lead to providers that do not respond to requests. Over 500 tracebacks have ended with no response so far this year, often when the traceback reaches an international provider. Some providers simply fail to respond entirely. Others, though less frequently, acknowledge the request but indicate that they are not obligated to respond and therefore choose not to. In either case, the ITG cannot continue the traceback.[9]

There are also times that the ITG process reaches a voice service provider that responds to the traceback request, but the provider refuses to identify their calling party customer, most often citing contractual restrictions. USTelecom appreciates the need to respect the commitments in contracts. However, when presented with clear evidence of illegal calling, there should be an expectation to disclose the source of the illegal calling party that originated the call. Indeed, as the Enforcement Bureau has recognized, voice service providers refusing to identify the source of unlawful traffic can reasonably be characterized as "non-cooperative."[10]

Accordingly, the Commission can best maintain the ITG's momentum, already enhanced by the Commission's announcement of the ITG as the official Traceback Consortium,[11] by requiring participation in traceback requests. A mandate would levy additional pressure on those providers that do not respond as well as those that choose not to cooperate – and provide

[9] In such circumstances, because there is no additional information upon which the ITG can rely, the ITG considers the non-responsive voice service provider to be the originating provider. *See USTelecom's Industry Traceback Group: Policies and Procedures* at 2 (Jan. 2020) (defining "non-cooperative voice service provider" to include a provided that "does not cooperate").

[10] *See Traceback Consortium Order* ¶ 28 ("We find that it is reasonable to characterize as 'non-cooperative' a voice service provider that refuses to identify the source of unlawful traffic.").

[11] *See generally id.*

another hook for enforcement when those providers hinder others' efforts to stop illegal robocalls. Importantly, any such mandate should apply to *all* voice service providers that are originating calls to U.S. numbers, and to *all* providers in the call path of such calls, including non-U.S. providers. With a mandate, the ITG will be in a position to catalogue which providers follow the requirement and which do not – information that the ITG can then make known to other providers and enforcement agencies. In this regard, a mandate would help the industry and the Commission more rapidly identify and isolate bad actor service providers knowingly carrying unlawful traffic or otherwise turning a blind eye to it. It also should make those providers that in good faith feel restricted by their existing contracts more comfortable in sharing information with the ITG, as sharing such information would be necessary to meet their legal obligation.[12]

The Commission's enforcement focus,[13] in conjunction with the efforts of other federal and state enforcers,[14] has already had a noticeable impact on increasing provider participation, including by non-ITG members. Any additional steps to increase active participation are welcome. The Commission adopting an affirmative – and expressly sanctioning the ITG, as the Traceback Consortium, to make these requests to expedite the process to address non-

[12] Voice service providers' contracts with their partners and customers should allow disclosing the identity of a party identified by the ITG as the source of illegal calls as part of the traceback process, consistent with any exceptions in the contract for potential illegal activity by the customer. USTelecom, however, understands that such sharing is not always clearly permissible under existing contracts, nor is it always viable to amend those contracts so that such sharing is clearly permissible. A new Commission requirement to participate in tracebacks should in almost all instances enable the provider to share information about illegal robocalls, even under their existing contracts.

[13] *See, e.g., John C. Spiller et al.*, Notice of Apparent Liability for Forfeiture, FCC 20-74 (rel. June 10, 2020).

[14] *See, e.g., FTC Warns Nine VoIP Service Providers and Other Companies against 'Assisting and Facilitating' Illegal Coronavirus-related Telemarketing Calls*, Mar. 27, 2020, https://www.ftc.gov/news-events/press-releases/2020/03/ftc-warns-nine-voip-service-providers-other-companies-against; *States of Arkansas, Indiana, Michigan, Missouri, North Carolina, Ohio, and Texas v. Rising Eagle Capital Group LLC et al.*, Plaintiffs' Original Complaint, Case No. 20-2021 (S.D. Tex., June 9, 2020).

cooperative voice service providers[15] – is one such important step.

B. Imposing Mitigation Obligations on Voice Service Providers that Originate Illegal Robocalls Would Disrupt the Flow of Such Calls

The Commission proposes to require all voice service providers to take effective steps to mitigate bad traffic when notified of that traffic by the Commission.[16] It also proposes to require voice service providers to take affirmative measures to prevent new and renewing customers from using their networks to originate calls.[17] USTelecom strongly supports voice service providers taking affirmative measures to stop robocalls. As the Commission recognizes, "[t]he most effective way of preventing illegal calls from reaching American consumers is by ensuring that those calls never originate on or enter the network."[18] Therefore, the Commission should require providers to implement an "appropriate robocall mitigation program" for traffic they originate, consistent with USTelecom's prior proposal in the Commission's Call Authentication Trust Anchor proceeding.[19] Such a requirement should be applicable to all originating voice service providers.

Beyond merely responding to traceback requests, providers who have been identified as the originating provider of illegal calls by the Commission – or by the ITG as the Registered Traceback Consortium – should take appropriate mitigation steps. More generally, voice service providers should take steps to investigate and prevent the continued carriage of any illegal traffic when made aware of such calls and they are in a practical position to mitigate such traffic. This is particularly important when a provider has been identified as the U.S. point of entry for illegal

[15] *See Fourth FNPRM* ¶ 97.

[16] *Id.* ¶ 98.

[17] *Id.* ¶ 101.

[18] *Id.*

[19] *See, e.g.*, Comments of USTelecom – The Broadband Association, WC Docket Nos. 17-97 & 20-67, at 3-13 (filed May 15, 2020) ("USTelecom *STIR/SHAKEN FNPRM* Comments").

traffic placed on to the U.S. public switched telephone network ("PSTN").[20]

The Commission, however, should not prescribe particular steps voice service providers should take to mitigate unlawful traffic when they become aware of it. There is no one-size-fits-all solution, and different circumstances may require different approaches and actions. Moreover, mandated and specific mitigation steps may quickly become obsolete as bad actors change their practices, and indeed, such any detailed requirements may offer bad actors a roadmap to evade robocall protections. Accordingly, the Commission should allow providers flexibility in how they address and ultimately mitigate illegal robocall traffic.[21]

USTelecom also agrees with the Commission that originating voice service providers should take affirmative measures to prevent their customers from placing illegal robocalls.[22] Again, rather than adopt prescriptive obligations, the Commission should allow providers flexibility to implement the appropriate measures based on the circumstances. Numerous providers already have implemented, or are committed to implement, various robocall detection and mitigation methods in their own networks and operations.[23] USTelecom's proposal that the Commission require voice service providers to certify that they have implemented an

[20] *See Fourth FNPRM* ¶ 98 (proposing to require all voice service providers to take effective steps to mitigate bad traffic when notified of that traffic by the Commission). As described further below, the Commission should impose a requirement on voice service providers to implement an "appropriate robocall mitigation plan" for any traffic they originate. By its very nature, any such requirement generally would include the obligation for providers to mitigate unlawful traffic on their network when they become aware of it.

[21] In the event that a provider is presented with repeated and substantial evidence of illegal calling through its network, it is even more critical that the provider takes appropriate mitigation steps. Accordingly, the Commission should establish an expectation that, when presented with evidence of repeated illegal calling through its network, the provider will take proactive steps to prevent the continued origination of such traffic and, where possible for international calls, prevent the calls from entering the PSTN.

[22] *See Fourth FNPRM* ¶ 101.

[23] *See, e.g., Anti-Robocall Principles for Voice Service Providers*, https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf (commitments to analyze and monitor network traffic, investigation suspicious calls and calling patterns, confirm the identity of commercial customers, and require traceback cooperation in contracts, among other principles).

"appropriate robocall mitigation program" for traffic they originate would achieve the Commission's aims by making sure that *all* voice providers are taking appropriate measures.[24]

The steps a given provider should take necessarily depend on the nature of the traffic it carries, its knowledge of its customer base, and numerous other factors. For instance, a provider with end users incapable of originating large volumes of calls should be permitted to certify that it has an appropriate program because the risk the provider's network will become part of an illegal robocaller's attack vector is low.[25] Other providers could take one or more of the following reasonable steps to avoid originating illegal robocalls, depending on the particular context:

- Confirming the identity of new commercial VoIP customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the general nature of the customer's business;
- Analyzing high-volume voice network traffic to identify and monitor patterns consistent with illegal robocall campaigns;
- Analyzing traffic for patterns of fraudulent calls, such as identifying short duration calls with low completion rates;
- Upon detection of a pattern consistent with illegal robocalls, or upon suspicion of illegal robocalling or illegal spoofing, seeking to identify the party using the network to originate, route, or terminate the calls, such as through a traceback investigation;
- Taking appropriate remedial action upon identifying the party originating, routing, or terminating illegal robocalls, such as suspending the party's ability to originate, route, or terminate calls on its network and/or notifying law enforcement authorities; and
- Providing prompt and complete responses to traceback requests from law enforcement and the ITG, as the Registered Traceback Consortium.[26]

Adopting affirmative robocall mitigation requirements would provide incentives for

[24] *See, e.g.*, USTelecom *STIR/SHAKEN FNPRM* Comments at 3-13.

[25] *Id.* at 8.

[26] *See id.* at 8-9. Then any service providers frequently cited as the origination source of illegal calls could be presumed by the Commission as having a deficient robocall mitigation program, if not presumed to be aiding or facilitating the origination of illegal traffic. *See id.* at 9.

providers to prevent illegal calls from originating on their network in the first instance, in addition to ensuring that they effectively mitigate traffic when they become aware that they originated that traffic or placed it on the U.S. PSTN through their network.[27]

III. THE COMMISSION SHOULD CONTINUE TO AFFORD SERVICE PROVIDERS FLEXIBILITY, INCLUDING BY EXTENDING THE REASONABLE ANALYTICS SAFE HARBOR TO NETWORK-LEVEL BLOCKING

The Commission appropriately recognized that service providers require flexibility to best adapt to, and address, evolving robocall threats in the *Third R&O*.[28] To that end, the Commission should look for ways to promote additional flexibility that will encourage and empower service providers to protect consumers from illegal robocalls. Extending the reasonable analytics safe harbor to network-based blocking is one such way.[29]

Network-based blocking is an important tool in a provider's arsenal to stop illegal calls. Network-based blocking specifically targets calls that are highly likely to be illegal, including those calls that the Commission authorized service providers to begin blocking in 2017[30] and other calls that providers have identified as highly likely to be illegal through a combination of analytics and network monitoring capabilities. These tools already are protecting consumers from billions of illegal calls[31] and a safe harbor would offer providers additional confidence to

---

[27] The Commission asks whether it should adopt these rules under section 201(b) of the Communications Act. *See Fourth FNPRM* ¶ 103. Reliance on section 201(b) is unnecessary. The agency can and should rely on authority under the Truth in Caller ID Act to impose the requirement to respond to traceback requests and section 4(b)(5)(c) of the TRACED Act for a robocall mitigation program requirement.

[28] *See Third R&O* ¶ 29 (flexibility needed in how to incorporate authentication in analytics); *id.* ¶ 50 (recognizing the need for flexibility to adapt to evolving call patterns); *id.* ¶ 59 (favoring flexibility rather than prescribing notification or other blocking requirements).

[29] *See Fourth FNPRM* ¶ 104 (proposing to extend the safe harbor based on reasonable analytics to cover network-based blocking).

[30] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and order and Further Notice of Proposed Rulemaking, CG Docket No. 17-59, FCC 17-151 (rel. Nov. 17, 2017) (authorizing blocking of calls from phone numbers on a Do-Not-Originate list and those that purport to be from invalid, unallocated, or unused numbers).

[31] *See, e.g.* CTIA, NCTA, and USTelecom Ex Parte, CG Docket No. 17-59, at 2 (filed July 14, 2020).

more broadly deploy these pro-consumer programs.[32]

Indeed, as the Commission recognizes, no reasonable consumer would want to receive the likely illegal calls targeted by network-level blocking.[33] The Commission therefore should make clear that not only is there no need for providers to offer a choice about such blocking,[34] but that there also is no need to notify consumers of such calls being blocked – as long as, as the Commission proposes, a service provider's network-based blocking program is managed with sufficient human oversight and network monitoring to ensure that blocking is working as intended.[35]

Many providers already are blocking illegal calls in their network, consistent with the Commission's prior rulings enabling them to do so. Extending the safe harbor for blocking based on reasonable analytics to network-level blocking would give those providers the confidence to deploy even more robust network-level programs – still targeting those calls highly likely to be illegal – as well as encourage providers not currently blocking calls highly likely to be illegal to do so.

The Commission also seeks comment on redress requirements for over-blocking and mislabeling of calls.[36] The Commission again should favor flexibility over prescriptive

---

[32] *See Fourth FNPRM* ¶ 104.

[33] *Id.* ¶ 105 ("We believe that no reasonable consumers would want to receive calls that are highly likely to be illegal….").

[34] *Id.* ("there is no need for consumers to have the opportunity to opt in or out" of network-level blocking of calls highly likely to be illegal).

[35] For other blocking based on reasonable analytics, most terminating voice service providers already provide subscribers, at their request, a list of the calls blocked as part of their commitment to provide transparency. It therefore is unnecessary for the Commission to adopt a formal blocked calls list requirement. *See id.* ¶ 111. However, if the Commission adopts its proposed requirement to provide a list of individually blocked calls, the Commission should make clear that the requirement does not apply to any network-based blocking targeting only those calls highly likely to be illegal, nor to any blocking of upstream bad actor providers under the *Third R&O*'s bad-actor safe harbor.

[36] *See id.* ¶¶ 107-109.

regulations. To that end, as USTelecom has previously suggested, the Commission should encourage calling parties and voice service providers to work together to develop industry best practices on appropriate mitigation steps to address claims of mislabeling or over-blocking.[37]

IV. CONCLUSION

The Commission has the opportunity to build on the *Third R&O* and other Commission initiatives to empower service providers and their partners to protect consumers from illegal and unwanted robocalls, while ensuring that *all* voice service providers – rather than just industry leaders – do their part to stop robocalls. To do so, the Commission should require all voice service providers to respond to traceback requests and to take affirmative steps to mitigate illegal robocalls when aware of and originating such calls. Moreover, all originating voice service providers should have to implement a robocall mitigation program and certify to the Commission that such a program is in place. The Commission also should look for ways to provide and enhance service providers' flexibility to protect their customers from illegal robocalls, including by extending the safe harbor for reasonable analytics to network-level blocking and looking to calling parties and voice service providers to work together to develop industry best practices on appropriate mitigation steps to address claims of mislabeling or over-blocking.

[37] *See* Reply Comments of USTelecom – The Broadband Association, WC Docket Nos. 17-97, 20-67, at 8-10 (filed May 29, 2019).

Respectfully submitted,

By: */s Joshua M. Bercu/*

Joshua M. Bercu
Vice President, Policy & Advocacy

Patrick Halley
Senior Vice President, Policy & Advocacy

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

August 31, 2020