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

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
	)	
Unlawful Robocalls, Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
	)	

COMMENTS OF
USTELECOM – THE BROADBAND ASSOCIATION

USTelecom – the Broadband Association ("USTelecom") [1] submits these comments in response to the Third Further Notice of Proposed Rulemaking ("Further Notice")[2] in the above-referenced dockets. USTelecom shares the Federal Communications Commission's ("Commission") goal to eliminate illegal robocalls and to help empower consumers to block such calls. Along with its members, USTelecom is working continuously to enhance our knowledge about the calls that traverse our members' respective networks in order to block illegal calls and provide consumers with more information about the calls they receive, and enhancing their ability to block or manage unwanted calls.

I. Introduction and Summary

As the FCC recently and correctly stated, "it is obvious that the volume of unwanted [robo]calls is reducing the value of telephony to anyone who makes or receives calls."[3] This is a

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

[2] *See Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51 (rel. June 7, 2019) (*Call Blocking Declaratory Ruling & Third Further Notice*).

[3] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Second Report and Order, FCC 18-177, CG Docket No. 17-59 at ¶ 4 (Dec. 2018) (describing the "multi-prong approach" to address the problem of unwanted calls).

significant problem for all stakeholders – consumers, small and large businesses, voice service providers, and government. USTelecom is deeply committed to working with all stakeholders to curtail the onslaught of illegal and unwanted robocalls and to provide solutions for consumers. We appreciate the Commission's recognition to date of the value of providing flexibility for industry to develop industry-led solutions to call blocking and call authentication. We also appreciate our collaborative relationship via the USTelecom Industry Traceback Group ("ITG") to identify the source of illegal robocalls and the commitment from the FCC to go after illegal robocallers, a function that will be enhanced with the deployment of the SHAKEN/STIR framework.

While the SHAKEN/STIR framework is not a silver bullet, it is an important tool in the robocall prevention toolbox that will help end illegal robocall campaigns by identifying the source of illegal robocalls which will greatly assist in traceback efforts. However, because the SHAKEN/STIR standard is not designed – and was never intended – to determine call intent or on a stand-alone basis or to be used to automatically keep calls from completing, limiting the applicability of a safe harbor for blocked calls to only those calls that fail SHAKEN/STIR verification is far too narrow. Some properly authenticated calls may in fact be illegal robocalls. And calls that have not been authenticated per the standard may be legitimate and important calls that should not be blocked. Thus, although it would be reasonable for the Commission to adopt a safe harbor based on whether a call fails verification by the terminating network, it should not adopt a safe harbor solely based on whether a call lacks authentication by the originating network.[4] However, the Commission should adopt a robust safe harbor that includes the use of reasonable analytics, which may include SHAKEN/STIR standards. Doing so will further incentivize voice

[4] *See Call Blocking Declaratory Ruling & FNPRM* at ¶ 53.

service providers to take more targeted actions to implement call blocking solutions and protect consumers.

USTelecom supports the Commission's objective to ensure legitimate calls are not blocked, in particular calls from emergency services agencies. However, USTelecom urges the Commission to proceed with caution before mandating a "Critical Calls List" because it is likely unnecessary with the implementation of SHAKEN/STIR combined with analytics and there are potentially significant risks that could emerge if illegal fraudsters gained access to such a list or are generally aware of publicly known numbers that may be on such a list.[5] Before requiring the establishment of such a list – with the complications and risks that could involve – the Commission should instead allow carriers to further deploy and refine call blocking efforts combined with the deployment of SHAKEN/STIR prior to determining whether such a list is necessary and appropriate. If the Commission were nevertheless to require the establishment of a Critical Calls List, then it should be a highly secure, non-public list centrally maintained by the Commission or a recognized public safety organization. A centrally maintained list would reduce substantial burdens that would be placed on emergency services agencies and voice service providers if they were all required to generate and maintain separate lists, lists that will inevitably lead to inconsistencies that would undermine public safety.

Regardless of their size, the Commission should require voice service providers acting as gateway providers (*i.e.*, providers that directly interconnect with international voice provider(s) and/or international customer(s)), to implement the SHAKEN/STIR framework. However, it is essential that any rules requiring the adoption of SHAKEN/STIR acknowledge the limitations of legacy networks and the challenges in implementing the IP-based standard for carriers with

[5] This could include administrative lines that are used in the event of 911 outages or poison control lines that are expected to be publicly known.

significant portions of TDM in their networks. The Commission has acknowledged the innovation regarding this limitation[6] and should allow such innovation to continue.

II. USTelecom and Its Members are Committed to Ending the Robocall Epidemic.

Identifying the source of and preventing illegal robocalls is a top priority for USTelecom. Our members are actively working on solutions to empower consumers with call labeling and blocking solutions, implementing call authentication protocols into their networks, and working collaboratively to identify the source of illegal calls through the USTelecom ITG.

First, industry has undertaken considerable efforts to deploy call authentication technologies, commonly referred to as SHAKEN/STIR[7] that will substantially diminish the ability of illegal robocallers to spoof caller-ID information. Major providers and other companies of all types and sizes are introducing this technology into their IP networks today, expecting to be authenticating IP-originated calls by year-end 2019.[8] Testing is already well underway, and the SHAKEN/STIR Governance Authority expects the framework to be launched in by the end of the year. Additional advances in blocking, labeling, and tools in combination with SHAKEN/STIR and its use with expanding data analytics will continue even after initial launch. With SHAKEN/STIR deployed, consumers will soon have more information available about the authenticity of the telephone number or with analytics the potential type of call they are receiving. Additionally, voice service providers will be able to more accurately identify the

[6] *See Call Blocking Declaratory Ruling & FNPRM* at ¶ 80 (acknowledging the work of the IETF to develop "out of band STIR").

[7] *Call Blocking Declaratory Ruling & FNPRM* at ¶ 21. (SHAKEN/STIR "is an industry-developed system to authenticate Caller ID and address unlawful spoofing by confirming that a call actually comes from the number indicated in the Caller ID, or at least that the call entered the US network through a particular voice service provider or gateway. Together, the Signature-based Handling of Asserted Information using toKENs (SHAKEN) framework and Secure Telephony Identity Revisited (STIR) make use of public key cryptography to provide assurances that certain information about the Caller ID transmitted with a particular call is accurate").

[8] Letters to multiple voice service providers from Chairman Pai on the status of SHAKEN/STIR deployment and carrier responses can be found at https://www.fcc.gov/call-authentication (last visited July 21, 2019).

source of calls, providing the key input to assist carrier call blocking analytics and to improve call traceback efforts.

Second, there are more tools available today than ever before for consumers to mitigate illegal or unwanted robocalls. A significant number of voice providers are increasingly integrating these tools into their networks and hundreds of applications are available to consumers on their smartphones.[9] Additional third-party products are appearing on the market, and voice providers and vendors are continuing work refining new and existing blocking, screening, and filtering tools.

Third, USTelecom's ITG is expanding its efforts to identify the source of illegal robocalls and working in close coordination with federal and state authorities to assist in enforcement efforts. Recently, we significantly enhanced our ability to traceback calls by further automating the process. The time needed to trace back illegal robocalls has now been reduced from weeks to days – sometimes even hours. As the Commission's Chief Technology Officer and Enforcement Bureau Chief noted in recent letters to providers encouraging participation in the USTelecom ITG, "neither government, nor industry, without the active assistance of the other, can hope to stem the flood of scam calls plaguing consumers across the country."[10] We agree and appreciate our active and collaborative relationship with the Commission's Enforcement Bureau and other law enforcement organizations to identify the source of illegal robocall campaigns and facilitate prompt action.

In all of these endeavors, the Commission has appropriately recognized that industry collaboration is essential for voice service providers to effectively and more promptly address

[9] *See e.g.,* Commissioner Rosenworcel Releases Responses to Call for Robocall Blocking Tools, Attachment (Jan. 28, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-355921A2.pdf.

[10] Press Release, FCC, FCC Calls on Network Voice Providers to Join Effort to Combat Illegal Spoofed Scam Robocalls (Nov. 6, 2018), https://docs.fcc.gov/public/attachments/DOC-354942A1.pdf.

robocalls. The Commission has emphasized the importance of "flexibility" and "a diversity of approaches" to stopping illegal and unwanted calls."[11] This approach enables industry to address new and emerging challenges efficiently and creatively, and we encourage the Commission to continue collaborating with industry while allowing innovation and reasonable flexibility to tackle this complex problem.

III. The Commission Should Broadly Define its Safe Harbor.

The adoption of a broad safe harbor for service providers is essential to ensure the fullest implementation of call blocking solutions to protect consumers. A robust safe harbor will provide voice service providers protection from liability for inadvertently blocking legal calls, while giving industry the flexibility and incentives it needs to continue innovating. While the SHAKEN/STIR framework will generally identify the source of illegal calls, it is ineffective by itself as the single input for voice service providers to make a sound determination whether to block a call. Instead, the Commission should adopt a safe harbor that includes the use of reasonable analytics, which may include SHAKEN/STIR standards in their call blocking tools.

A. The SHAKEN/STIR Framework is an Important Tool Against Robocalls, But Was Not Designed to be the Sole Basis for Call Blocking Determinations.

SHAKEN/STIR is an important tool that promises to be a critical component to industry's multi-pronged strategy to fight against the onslaught of robocalls. However, it is an insufficient basis alone for voice service providers to determine whether to block a call. The SHAKEN/STIR framework will significantly advance industry's and the Commission's shared goal of protecting consumers from illegal robocalls through better analytics and enhanced traceback capabilities. While deployment of SHAKEN/STIR standards alone is not a remedy to the robocall problem, these standards will improve the reliability of the nation's communications system by better

[11] *Call Blocking Declaratory Ruling & FNPRM* at ¶ *34.*

identifying traffic, and more rapidly locating the source of illegal calls. A SHAKEN/STIR framework will help prevent illegal robocalls by helping to reintroduce trust into the caller ID framework and more rapidly identifying the source of illegal robocalls.

But it is critical to remember that the SHAKEN/STIR standard is not designed, and has never been intended, to determine caller intent or in and of itself to keep calls from completing. According to the Governance Authority – the Alliance for Telecommunications Industry Solutions ("ATIS"), the SHAKEN standard is designed to achieve two narrow goals: 1) identify the originating provider of a call, and 2) authenticate the caller ID information associated with a particular call.[12] The ATIS-approved standard defines the protocol as one "for the authentication and assertion of a telephone identity by an originating service provider and the verification of the telephone identity by a terminating service provider."[13] Since the SHAKEN/STIR framework does not provide insight to the nature or content of a call (*i.e.*, whether a call is legal or illegal, legitimate or fraudulent, wanted or unwanted), it is an insufficient basis alone for voice providers to determine whether to block a call.

B. A Broad Safe Harbor Should Be Adopted That Includes Reasonable Analytics.

A safe harbor for voice service providers that choose to block calls based solely on failed Caller ID authentication under the SHAKEN/STIR framework is too narrow. For the reasons discussed above, particularly in the early stages of SHAKEN/STIR deployment, blocking calls by relying only on whether a call has been authenticated is very problematic and ill-advised. Some properly authenticated calls may in fact be illegal robocalls. And calls that have not been authenticated per the standard may be legitimate and important calls that should not be blocked.

[12] ATIS & SIP Forum, Joint ATIS/SIP Forum Standard — Signature-Based Handling of Asserted Information Using toKENs (SHAKEN) at 3 (2017), https://www.atis.org/stiga/resources/docs/ATIS-1000074.pdf (*SHAKEN Report*).

[13] *Id*.

Thus, the Commission should not adopt a safe harbor based solely on whether a call lacks authentication.

Instead, the Commission should broadly define its safe harbor to provide protections for voice service providers that implement SHAKEN/STIR and that follow reasonable practices, based on analytics that may include SHAKEN/STIR standards, in their call blocking and labeling tools. Such an approach will incentivize more voice providers to adopt the SHAKEN/STIR standard and utilize the information, while also increasing more accurate and effective call blocking and labeling. While the SHAKEN/STIR authentication framework alone is an insufficient basis for the Commission's safe harbor, including it as an element in a broader safe harbor based on reasonable analytics would strongly encourage voice service providers to deploy call blocking tools to their customers and increase the likelihood of voice service providers implementing default call blocking solutions. Consistent with this approach, the North American Numbering Council ("NANC") Call Authentication Trust Anchor Working Group envisioned a safe harbor as including both the SHAKEN/STIR standard, and reasonable analytics.[14] A broader, more robust safe harbor that includes reasonable analytics will enable voice service providers to more accurately assess the likely content of a call, while also encouraging more voice service providers to deploy call-blocking tools to their customers. Reasonable analytics in conjunction with SHAKEN/STIR authentication, as appropriate, are far better suited to making determinations about wanted versus unwanted calls than simply SHAKEN authentication alone.

The safe harbor should also broadly apply to all call blocking tools, whether the solutions are provided at the carrier network level or consumer-facing tools, because both are crucial in the

[14] The North American Numbering Council (NANC) Call Authentication Trust Anchor Working Group (CATA WG), Report on Selection of Governance Authority and Timely Deployment of SHAKEN and STIR, at 14 (2018), http://nancchair.org/ docs/mtg_docs/May_18_Call_Authentication_Trust_ Anchor_NANC_Final_Report.pdf. ("A safe harbor for unintended blocking or mis-identification of the level of trust for individual calls would provide a strong incentive for communications service provider adoption of SHAKEN, particularly where analytics are overlaid on the framework. Such liability protection may override reluctance to participate in SHAKEN, particularly in its early stages").

fight against robocalls. Regardless of whether a call is blocked by a carrier within its network (which would be unnoticed by the consumer as they will have taken no affirmative steps to enable such blocking) or by a consumer-facing application or service, carriers should be expected to use some data analytics when making the determination to block the call. It should not matter what form the call blocking takes as long as such analytics are reasonable, which should be enough to qualify for the safe harbor. Finally, the Commission should also consider limiting the availability of a safe harbor to those voice service providers that cooperate in call tracebacks through the USTelecom Industry Traceback Group.[15] Doing so will promote broader cooperation among voice service providers in call tracebacks. A broad safe harbor that is based on reasonable analytics will strongly encourage voice service providers to deploy smarter and more effective call blocking tools and services than if the risk of liability for inadvertent blocking or labeling errors hangs over them.

IV. The Commission Does Not Need to Adopt a "Critical Calls List" at This Time, But if a List Is Created It Should be Centrally Maintained.

USTelecom naturally agrees that emergency calls should not be blocked.[16] However, USTelecom urges the Commission to proceed with caution before requiring the establishment of a Critical Calls List. Developing and maintaining such a list is a complex task, and it is unnecessary with the implementation of SHAKEN/STIR combined with analytics. Additionally, there are significant risks that could emerge if illegal fraudsters gained access. The implementation of SHAKEN/STIR and analytics technology should very likely address the Commission's concern without the need for a list. Before requiring the creation of a critical calls list, the Commission should review the results of carrier call blocking efforts combined with the deployment of SHAKEN/STIR to determine whether such a list is actually necessary. Once

[15] *Call Blocking Declaratory Ruling & FNPRM* at ¶ 55.

[16] *Id.* at ¶ 63.

SHAKEN/STIR is implemented, voice service providers will be able to effectively identify and address spoofed calls from all numbers, including numbers used by emergency services agencies. Thus, voice service providers that have implemented SHAKEN/STIR and have deployed call analytics capabilities should be able to prevent fraudulently spoofed emergency calls from being delivered without the need for such a list. On the other hand, a critical calls list that requires voice service providers to allow the completion of calls from certain numbers could result in an obligation on voice service providers to allow calls to complete that they know are from spoofed numbers. This would be contrary to the Commission's and the industry's shared objectives.

USTelecom recognizes the potential security risks of maintaining a central critical calls list. In the event that a list was breached, it would create two significant problems. First, it would immediately render moot the list's protections for emergency call centers. Second, because robocallers would know that these numbers are on the critical call list, they would be encouraged to start spoofing these numbers to evade network blocking. This in turn would undermine the public confidence in and reputation of these emergency call centers by associating their legitimate numbers with criminal activities. Accordingly, the Commission should establish a list only if it has a fuller record to show that it would be necessary to avoid blocked calls without opening a backdoor to fraudsters. Such a determination is best made after studying the experience after SHAKEN/STIR has been in place. It is important to note, however, that the Commission's consideration of this issue should not delay the adoption of a safe harbor. Regardless of whether or how the Commission resolves this topic, it should promptly adopt a safe harbor.

If the Commission nevertheless were to require the creation of a critical calls list, then it must of course ensure that it is kept secure and non-public[17] to avoid unlawful spoofing.[18] The

[17] Keeping a list non-public may be difficult since many emergency services numbers are public for the sake of providing the emergency service.

[18] *See Id.*at ¶ 68.

Further Notice asks whether a “Critical Calls List be centrally maintained” or if “each voice service provider” should maintain their own list.[19] If the Commission requires the creation of a list, either the Commission or a recognized national public safety organization should be responsible for its creation and maintenance. Regardless of who is ultimately responsible for developing, maintaining, and managing the list, it should be a single, centralized, national list. The creation of separate state, regional, or type lists would be administratively inefficient and unreliable for both industry and public safety entities. If each voice service provider maintained its own list, every critical communications entity would have to continually reach out to each voice service provider to confirm they are on each provider’s list – a massive and inefficient task. When initially established, each public safety entity would also have to field dozens of calls from various voice service providers all seeking access to the same information. In addition, in instances where public safety entities need to update or change their lists (*e.g.*, by adding or removing telephone numbers), they would need to contact multiple providers to perform these updates.

Separate lists maintained by several entities would also lack uniformity and discrepancies would likely exist that could cause harm or confusion. Such an environment would mean that public safety entities making emergency calls could be blocked on some networks (where their numbers are not listed), but not others (where their numbers are listed). This would create an unpredictable and unreliable calling environment for public safety agencies, since their outbound emergency calls could be subject to disparate treatment across various networks. In addition, the significant penetration of mobile phones in the residential marketplace (more than half of today’s households are wireless only) could also introduce problematic dynamics in the operation of a critical calls list particularly for smaller, local public safety organizations. For example, while a

[19] *Id.* at ¶ 65.

local PSAP may have a small population to which it may need to make critical calls, it would nevertheless need to ensure that its outbound numbers are listed with every wireless provider in the country. This could prove challenging to smaller, less sophisticated, government agencies, and could put outbound emergency calls at risk from ever reaching consumers.

V. Voice Service Providers Accepting International Traffic Should be Required to Implement the SHAKEN/STIR Caller ID Authentication Framework.

The Further Notice asks if there is another threshold for "major voice service provider" that could be used.[20] Regardless of their size, the Commission should require voice service providers acting as gateway providers (*i.e.*, providers that directly interconnect with international voice provider(s) and/or international customer(s)) to implement the SHAKEN/STIR standard.

Signing calls entering voice service providers' networks can also assist with legacy TDM networks that do not work with the SHAKEN framework at this time. The full value of SHAKEN requires the use of end-to-end IP networks.[21] Although there may be capabilities that allow TDM networks to take advantage of SHAKEN information, these TDM networks may be further limited, such as those not capable of providing Caller ID or supporting Advanced Intelligent Network ("AIN") functionality. This is not only challenging for smaller and rural carriers, but it will also affect many major voice service providers that have hybrid networks or maintain any significant portions of their network using legacy technology.

In the SHAKEN/STIR framework, voice service providers can give full, partial, or gateway attestation to the calls they sign. Full attestation indicates the greatest certainty that the caller is authorized to use the number, while partial and gateway attestation indicate less certainty but indicates where the call originated on the network.[22] Major voice providers are already on

[20] *Call Blocking Declaratory Ruling & FNPRM* at ¶ 73.

[21] *See generally Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Inquiry, 32 FCC Rcd 5988 (2017) (*Call Authentication NOI*) at ¶ 7-8).

[22]ATIS & SIP Forum at 8. ("Attestation under the SHAKEN framework can take three basic forms. Full attestation requires that the signing voice service provider: 1) is responsible for the origination of the call onto the network; 2)

record with the Commission regarding their commitment to deploy the SHAKEN/STIR framework as early as the end of 2019.[23] The low volume of high risk robocalls across top U.S. carrier networks suggest robocallers continue to capitalize on networks and numbering resources from non-Tier-1 carriers.[24] The Commission should consider whether to apply this standard to non-Tier 1 providers since the major voice providers are not generating the majority of the illegal robocall traffic. Smaller voice service providers may have only a handful of subscribers (thereby falling outside the scope of the Commission's proposed definition), but nevertheless may generate a significant and disproportionate volume of traffic from overseas relative to their size. Applying this standard would ensure that calls entering through a gateway provider are appropriately signed (*i.e.*, gateway attestation). This would enable the Commission, individual voice service providers, and/or USTelecom's ITG to immediately identify the ingress voice service provider for these calls into the United States, thereby expediting and improving more rapid mitigation efforts.[25] For example, iconectiv states that "[s]tandard implementation of the

"[h]as a direct authenticated relationship with the customer and can identify the customer;" and 3) "[h]as established a verified association with the telephone number used for the call." By contrast, partial attestation only requires that the first two requirements be met. Finally, gateway attestation is the most limited form of attestation, requiring only that the signing voice service provider both be "the entry point of the call into its VoIP network" and have "no relationship with the initiator of the call (e.g., international gateways)").

[23] *See, e.g.*, Letter from Joan Marsh, Executive Vice President, Regulatory and State External Affairs, AT&T Communications, to Ajit Pai, Chairman, FCC, WC Docket No. 17-97 (filed Nov. 19, 2018) (AT&T Nov. 19th Letter); Letter from Tony Werner, President of Technology and Product, Comcast Cable, to Ajit Pai, Chairman, FCC, WC Docket No. 17-97 (filed Nov. 19, 2018) (Comcast Nov. 19th Letter); Letter from Jennifer Hightower, Senior Vice President and General Counsel, Cox Communications, to Ajit Pai, Chairman, FCC, WC Docket No. 17-97 (filed Nov. 19, 2018) (Cox Nov. 19th Letter); Letter from Kathleen O'Brien Ham, Senior Vice President, Government Affairs, T-Mobile, to Ajit Pai, Chairman, FCC, WC Docket No. 17-97 (Nov. 19, 2018) (T-Mobile Nov. 19th Letter); Letter from Joseph J. Russo, Vice President, Global Network Operations, Verizon, to Ajit Pai, Chairman, FCC, WC Docket No. 17-97 (filed Nov. 19, 2018) (Verizon Nov. 19th Letter).

[24] Transaction Network Services, Annual Report (2019), https://tnsi.com/tns-report-finds-only-10-of-high-risk-robocalls-come-from-tier-1-carriers. ("While the top six U.S. carriers (AT&T, CenturyLink, Comcast, Sprint, T-Mobile and Verizon) account for three-fourths of total call volume, only 10% of high risk illegal robocalls now originate from numbers owned by these six carriers").

[25] Moreover, SHAKEN and STIR provides non-repudiation: since only the carrier holding the private key can have signed an attestation validated with the public key, we know definitively which carrier has signed the attestation. This greatly improves the traceback process, as the public key directly and definitively identifies the originating carrier.

SHAKEN/STIR technique worldwide would dramatically mitigate the international robocall problem."[26]

The Commission could also consider an additional requirement obligating gateway providers to pass such international traffic to a downstream provider that has implemented the SHAKEN/STIR framework. This will help to ensure that any gateway attestation is not stripped out by a provider's network that does not have SHAKEN capability. The Commission implemented a similar framework in its Rural Call Completion Order. There, the Commission required any intermediate provider to register in its Intermediate Provider database in order to ensure call integrity.[27] A similar approach adopted in the SHAKEN context would ensure a heightened degree of transparency and accountability into any given call path.

USTelecom has been consistently supportive of the Commission's recognition of the benefits of providing flexibility to voice service providers in adopting solutions to address robocall challenges.[28] Many of USTelecom's members have publicly committed to deploying SHAKEN/STIR and are actively taking steps to meet those commitments. The vast majority of illegal robocalls are interstate long-distance and international calls, which primarily transit the IP networks of voice communications providers that are in the process of implementing SHAKEN/STIR. Significant progress and innovation has been made. At the same time, we understand the Commission's inquiry into potential requirements to ensure broader adoption of

[26] iconectiv Comments, CG Docket No. 17-59 (rec. June 19, 2018) at 4. (iconectiv notes that implementation of SHAKEN/STIR in the U.S. will allow traceback of all calls to the point of entry onto the U.S. network for international calls. However, they point out that there could still be significant difficulty tracing international calls back to their point of origin absent international implementation of the standards.)

[27] *Rural Call Completion*, WC Docket No. 13-39, Second Report and Order and Third Further Notice of Proposed Rulemaking, FCC 18-45, (rel. Apr. 17, 2018) (RCC FNPRM) at ¶ 69. ("The RCC Act further requires that intermediate providers register with the Commission, and precludes covered providers from using intermediate providers who are not registered. These requirements will help to ensure that covered providers only use responsible intermediate providers and can identify intermediate providers in the call path").

[28] *See supra* at 4-5; *see e.g. Call Blocking Declaratory Ruling & FNPRM* at ¶ 80 (acknowledging the work of the IETF to develop "out of band STIR").

the SHAKEN/STIR framework. If the Commission determines that it will require adoption of SHAKEN/STIR, it is essential that the rules acknowledge the limitations of legacy networks and the challenges in implementing the standard for carriers with significant portions of TDM in their networks. As the Further Notice states, "SHAKEN/STIR as developed is intended for IP-based networks, and thus, is less effective for calls that originate, terminate, or transit across TDM networks and does not work at all for calls that exclusively traverse TDM networks."[29] Any rules must acknowledge these limitations and the costs, challenges, and impact on innovation that a mandate will impose on such carriers.

VI. CONCLUSION

USTelecom appreciates that the Commission's proposals in this proceeding provide voice service providers with important flexibility to address the robocall problem. While the SHAKEN/STIR framework is not a silver bullet, it could help stop robocallers by identifying the source of illegal robocalls while greatly enhancing traceback efforts. However, it is an insufficient basis alone for voice service providers to determine whether to block a call. USTelecom encourages the Commission to establish a robust broad safe harbor that uses reasonable analytics, to proceed with caution before requiring the establishment of a Critical Calls list, and to require voice service providers acting as gateway providers accepting international traffic to implement the SHAKEN/STIR Caller ID authentication framework. Finally, if the Commission adopts rules requiring the implementation of SHAKEN/STIR, it is essential that the limitations of legacy TDM network are appropriately addressed to allow for continued innovation.

[29] *Call Blocking Declaratory Ruling & FNPRM* at ¶ 80.

Respectfully submitted,

By: Farhan Chughtai

Farhan Chughtai
Director, Policy & Advocacy
USTelecom Association
601 New Jersey Avenue, N.W.
Suite 600
Washington, D.C. 20001
(202) 551-0761

July 24, 2019