Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

REPLY COMMENTS OF CTIA

CTIA respectfully submits these reply comments in response to the Notice of Inquiry

("NOI") released by the Federal Communications Commission ("FCC" or "Commission") in the

above-captioned proceeding seeking input on methods to authenticate telephone calls.[1]

I.   INTRODUCTION AND SUMMARY

CTIA and the entire wireless industry are actively developing a robust call authentication

framework to combat illegal robocalls and other spoofed calls. As Chairman Pai noted, "the

wireless industry has made strides in attacking this problem."[2] The wireless industry has also

heard the Chairman's request "to engage deeply in [the] effort to create a call authentication

system—a sort of digital fingerprint for every phone call [that] would give consumers

meaningful relief from robocalls,"[3] and is committed to this effort. CTIA and its members have

led multi-pronged efforts to reduce illegal robocalls, including in the industry *Robocall Strike*

Force. This includes accelerated work on authentication protocols, traceback, blocking, and root

cause removal. Additionally, industry has provided a broad variety of tools to consumers to help

block robocalls, including applications on smartphones, advisories on carrier websites, and call

---

[1]   *See Call Authentication Trust Anchor*, Notice of Inquiry, 32 FCC Rcd. 5988 (2017)
("NOI").

[2]   Ajit Pai, Chairman, FCC, Keynote Address at the Mobile World Congress Americas at 5
(Sept. 12, 2017), http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0912/DOC-
346666A1.pdf.

[3]   *Id.*

screening capabilities.[4] Protecting consumers through technical innovation and adaptability has

been the industry's hallmark in responding to the constantly changing landscape.

To promote meaningful solutions that can help in the near term, the Commission should

support the work being done right now by ATIS and the private sector to address illegal

robocalls. It should avoid actions, such as regulatory mandates, that could delay or distract from

this important effort. Indeed, the record shows broad support for the SHAKEN/STIR

framework.[5] It also shows a general consensus that the FCC should not mandate a particular

solution or action at this time, but promote ongoing work in these areas. The record likewise

supports a hybrid governance model and Commission efforts to promote call authentication

abroad. Finally, commenters agree that standards bodies should continue to address the other

issues raised in the NOI, such as privacy, security, and legacy networks.

II. COMMENTERS SUPPORT VOLUNTARY IMPLEMENTATION OF CALL AUTHENTICATION FRAMEWORKS.

The record shows strong support for SHAKEN/STIR. This should come as no surprise,

as "the framework has broad industry support."[6] SHAKEN/STIR is "promising,"[7] provides the

most "viable and reasonable long-term solution[] for Internet Protocol ("IP") based voice

---

[4]   Industry Robocall Strike Force at 14-18 (Apr. 28, 2017) ("Strike Force Report Update"), *attached to* Letter from ACT-The App Association, Alliance for Telecommunications Industry Solutions ("ATIS"), CTIA, and USTelecom, to Marlene H. Dortch, Secretary, FCC, CG Docker No. 17-59 (filed Apr. 28, 2017), https://www.fcc.gov/file/12311/download.

[5]   *See, e.g.,* Comments of Neustar, Inc., WC Docket No. 17-97 at 1 (filed Aug. 14, 2017) ("Neustar Comments"); NTCA Comments at 2; Comments of NCTA – The Internet & Television Association, WC Docket No. 17-97 at 1 (filed Aug. 14, 2017) ("NCTA Comments"); Comments of the Voice on the Net Coalition, WC Docket No. 17-97 at 1 (filed Aug. 14, 2017) ("VON Comments").

[6]   Comments of Comcast Corporation, WC Docket No. 17-97 at 2 (filed Aug. 14, 2017) ("Comcast Comments") (quoting Strike Force Report Update at 5).

[7]   Comcast Comments at 2.

communications,"[8] and may "facilitate the ability of a variety of stakeholders to identify illegal robocalls and the sources of untrustworthy communications."[9] By requiring carriers to receive certificates from trusted services that authenticate outgoing calls, SHAKEN/STIR offers greater accountability and transparency, making it possible to trace back, in a more rapid manner, the source of illegal robocalls so they can be blocked and/or the originator identified and subject to possible enforcement action. In this way, it provides an important, standardized, Internet-based tool.

Industry completed the standard in January 2017 and is in the process of implementing it. The standard needs time to evolve and adapt as industry gains experience with its use and effectiveness in combating illegal robocalls. Recently, industry finished designing a governance model and certificate management framework, and is now developing "deliverables to address call display issues, implementation guidance/best practices, deployment metrics," and further defining the policy administrator role.[10]

Although some efforts may be completed by the end of 2017, there is ongoing work on call authentication, making it premature to pursue any mandate at this point.[11] The FCC can readily dismiss Consumers Union's call to *require* all carriers to implement call authentication

---

[8]   Comments of NTCA – The Rural Broadband Association, WC Docket No. 17-97 at 2 (filed Aug. 14, 2017) ("NTCA Comments").

[9]   Comments of the USTelecom Association, WC Docket No. 17-97 at 2 (filed Aug. 14, 2017) ("USTelecom Comments").

[10]   Comments of the Alliance for Telecommunications Industry Solutions, WC Docket No. 17-97 at 2 (filed Aug. 14, 2017) ("ATIS Comments").

[11]   *See, e.g.*, NCTA Comments at 2-3; Neustar Comments at 1; NTCA Comments at 5; Comments of Telcordia Technologies d/b/a iconectiv, WC Docket No. 17-97 at 2 (filed Aug. 14, 2017) ("iconectiv Comments").

by the end of 2018.[12] Call authentication models like SHAKEN/STIR are in development and

testing, thus are not ready for mandatory adoption.[13] This is especially true as networks are

transitioning to IP-based technology.[14] As CTIA discussed, a mandate may create risks that

could hinder innovation.[15] Further, call authentication requires widespread global adoption to be

effective, so mandating call authentication in the U.S., while most countries have yet to engage

in any effort, will unnecessarily burden U.S. operators and may drive more bad actors overseas,

exploiting difficulties in verifying inbound calls.

A mandate is not needed to encourage carriers to implement call authentication. Carriers

are aware of the frustration caused by illegal robocalls and are developing tools to help stop

them. As ATIS stated, "market forces are sufficient to encourage the continued adoption of

[these protocols]," and "[s]ervice providers are already highly incented to provide call

authentication to meet the needs of consumers in the competitive marketplace."[16] The industry

needs flexibility to use and refine the SHAKEN/STIR framework and other approaches.

Cost concerns also make a mandate ill-advised now. Commenters noted the high cost of

call authentication, particularly for small providers.[17] The Commission should not burden

---

[12]   Comments of Consumers Union, Consumer Action, Consumer Federation of America, National Association of Consumer Advocates, National Consumer Law Center, on behalf of its low-income clients, Public Citizen, and Public Knowledge, WC Docket No. 17-97 at 2-3 (filed Aug. 11, 2017) ("Consumers Union Comments").

[13]   VON Comments at 2.

[14]   NCTA Comments at 2; VON Comments at 2-3.

[15]   Comments of CTIA, WC Docket No. 17-97 at 7 (filed Aug, 14, 2017) ("CTIA Comments").

[16]   ATIS Comments at 3; NTCA Comments at 5-6; Comments of Transaction Network Services, WC Docket No. 17-97 at 4 (filed Aug. 14, 2017) ("TNS Comments").

[17]   *See, e.g.*, Comments of the American Cable Association, WC Docket No. 17-97 at 2 (filed Aug. 14, 2017); NTCA Comments at 5-6.

carriers with costly mandates, and it certainly should not require carriers to offer call authentication for free, as urged by Consumers Union.[18] Some providers may choose to offer call authentication services bundled with their service offerings at low or no cost as a differentiator, but there is no need for the Commission to dictate how carriers set prices and recover costs for this service.

Finally, the Commission need not "direct service providers and vendors to participate in the ATIS Robocalling Testbed," as suggested by Neustar.[19] The testbed facilitates interoperability testing for SHAKEN/STIR. The testbed is important, but interoperability will be worked out with collaboration and consensus approaches. Mandating a particular approach or participation in the testbed effort would be counterproductive. A number of providers and vendors already participate, and ATIS is encouraging additional participation. ATIS itself did not request compulsion, so forcing providers to test call authentication solutions in one particular way would be inappropriate.

III. THE RECORD SUPPORTS A HYBRID GOVERNANCE MODEL AND THE RECOMMENDATIONS OF ATIS REGARDING IMPLEMENTATION.

The record shows consensus support for a hybrid governance model in which industry leads with FCC support.[20] This structure offers flexibility to quickly address evolving threats and adapt to ongoing learning and innovation without the need to go through a lengthy rulemaking or regulatory process.[21] It also maintains industry leadership, which has already fostered "significant progress on the SHAKEN/STIR framework without the need for Commission

---

[18]   Consumers Union Comments at 3-4.

[19]   Neustar Comments at 4-5.

[20]   *See, e.g.,* Comcast Comments at 7-8; NCTA Comments at 3.

[21]   Comcast Comments at 8.

involvement."[22]

Although some commenters opined that one of the existing numbering administrators should serve as the policy administrator,[23] the lack of clear synergies between numbering and call authentication do not make any one existing entity an obvious choice for this role. As ATIS notes, "the role envisioned for the call authentication policy administrator is significantly different than other existing databases or programs such that there may not be significant advantages to [using an existing administrator]."[24] It is also premature to consider methods for selecting or managing administrators,[25] as such decisions should be shaped by standards bodies.[26]

CTIA supports ATIS' recommendation that service providers should have an Operating Company Number ("OCN") to sign calling party information.[27] Although other models[28] might one day be appropriate, at this point, using OCNs is "a reliable and clear criteria for the initial deployment of SHAKEN that will help to prevent bad (or careless) actors from undermining the

---

[22]   NCTA Comments at 2.

[23]   Neustar Comments at 5-8; NTCA Comments at 5.

[24]   ATIS Comments at 11.

[25]   TNS Comments at 4 (suggesting that selection of the governance authorities "be open to competitive bid").

[26]   Robocalling: Secure Telephone Identity Governance Authority (STI-GA) Proposal at 3-5, *attached to* Letter from Thomas Goode, General Counsel, Alliance for Telecommunications Industry Solutions, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 (filed June 30, 2017) (noting that ATIS is still working on developing and defining the policy administrator and governance authority roles).

[27]   Joint ATIS/SIP Forum Standard – Signature-Based Handling of Asserted Information Using toKENs: Governance Model and Certificate Management, Appx. A (July 11, 2017), https://access.atis.org/apps/group_public/download.php/35256/ATIS- 1000080.pdf.

[28]   Neustar Comments at 9 (commenting that the proposal to only permit service providers with an OCN to sign calling party information will prove to be too restrictive and the FCC should instead permit the PA and the NANC to develop an appropriate criteria).

system."[29] In the future, "the industry could leverage SHAKEN operational experience as it evolves the framework to the broader set of call originators and support non-OCN stakeholders,"[30] but now is not the time for the Commission to promote other models that could distract from rolling out existing frameworks. In a similar vein, CTIA agrees that certifying each individual telephone number or number ranges, as opposed to certifying service providers, will likely delay implementation, so such a proposal should wait until after initial deployment.[31] The Commission should embrace innovation, and let operators work out the details and make improvements over time.

IV.   INTERNATIONAL COOPERATION IS NEEDED TO HAVE EFFECTIVE CALL AUTHENTICATION.

Commenters discussed the importance of promoting call authentication abroad, as most illegal robocalls originate overseas. CTIA agrees that "the Commission should encourage other countries to adopt call authentication frameworks that are compatible with the framework envisioned for the U.S."[32] The Commission should "leverage the results of the consensus authentication approach developed by ATIS, the SIP Forum and the IETF, and work to socialize and promote this effort with other international stakeholders and governments."[33]

Promoting call authentication overseas is the only realistic way to address the goal of creating a call authentication system that "protect[s] consumers from spoofed calls originating overseas."[34] It is naïve to suggest, as Consumers Union does, that U.S. operators alone can

---

[29]   ATIS Comments at 13-14.

[30]   iconectiv Comments at 12-13.

[31]   Neustar Comments at 9-10; iconectiv Comments at 7-8.

[32]   ATIS Comments at 17.

[33]   USTelecom Comments at 3.

[34]   Consumers Union Comments at 4.

address all robocalling traffic originating overseas. It is not a matter of simply using technology; authenticating calls that originate overseas requires other countries to improve their approaches and build trust. Without international adoption, bad actors will simply move their origination points elsewhere to work around the U.S. system. Thus, by promoting call authentication overseas, the FCC will help protect consumers from robocalls and spoofed calls originating abroad.

V.   REMAINING ISSUES SHOULD BE ADDRESSED BY STANDARDS BODIES.

Many issues in the NOI – such as privacy, security, and the implications for SS7 – are being addressed by industry and should not become a barrier to promoting the SHAKEN/STIR framework now.[35] The standards process has considered some of these issues, such as SS7, and the Commission should not let concerns about legacy systems stymie innovation.[36]

VI.   CONCLUSION

CTIA appreciates the Commission's support for call authentication, which is an important tool in the fight against illegal robocalls and other spoofed calls. The wireless industry continues to lead and develop innovative solutions to reduce these calls. These solutions are being deployed and show great promise. In the meantime, CTIA urges the Commission to avoid premature mandates and allow standards bodies to continue their work. The Commission also

---

[35]   CTIA Comments at 9-13.

[36]   Because SHAKEN/STIR is designed for IP-based networks, it cannot cover wireline, legacy, or TDM/SS7-based networks, as Consumers Union asks the FCC to mandate, and Neustar suggests should be pursued. *See* Consumers Union Comments at 4; Neustar Comments at 8. ATIS is correct that creating an authentication framework for legacy networks is not feasible, as most SS7/TDM equipment has been discontinued and manufacturers are leaving the marketplace. This would add unnecessary complexity and certainly delay implementation of SHAKEN, while yielding little in return. ATIS Comments at 6-7.

should promote call authentication abroad, because this is a truly global challenge. The wireless

industry looks forward to continuing its leadership in this effort and the Commission's support.

Respectfully submitted,

/s/ Scott Bergmann

Scott Bergmann
Vice President, Regulatory Affairs

Thomas C. Power
Senior Vice President, General Counsel

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

September 13, 2017