Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 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

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Matthew Gerst
Vice President, Regulatory Affairs

Sarah Leggin
Director, Regulatory Affairs

CTIA
1400 16th Street, NW
Suite 600
Washington, DC 20036
(202) 736-3200
www.ctia.org

July 24, 2019

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 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

COMMENTS OF CTIA

CTIA[1] respectfully submits these comments in response to the Federal Communications Commission's ("FCC" or "Commission") Further Notice of Proposed Rulemaking ("FNPRM") on further steps to enable voice service providers to offer robocall-blocking services.[2]

I. INTRODUCTION AND SUMMARY.

CTIA's member companies recognize that illegal and unwanted robocalls are a problem for American consumers,[3] and are committed to protecting consumers, providing them with tools to determine which calls they do not want to receive, and working collaboratively with policymakers to address the litany of issues these calls present. Wireless service providers, together with others in the voice service industry, are constantly innovating and acting to stay ahead of the fraudsters and scammers who are polluting the voice network with illegal and

[1] CTIA – The Wireless Association® ("CTIA") (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51 (rel. June 7, 2019) ("*FNPRM*").

[3] *FNPRM*, ¶¶ 3–15.

unwanted calls. This is why voice service providers have led the way in developing and deploying SHAKEN/STIR, which CTIA's member companies are aggressively testing and launching this year, to help consumers regain trust in caller identification information. In addition, voice service providers are using a variety of tools to mitigate the daily threat from *billions* of illegal and unwanted robocalls, among other initiatives.[4]

In addition to these efforts, CTIA and its member companies welcome the Commission's help in combating illegal and unwanted robocallers and regaining consumer trust in voice services. As Chairman Ajit Pai has recognized, a "multi-pronged approach" is necessary "to battle the noxious intrusion of illegal robocalls,"[5] and the wireless industry stands ready to launch new lines of attack alongside the Commission. If adopted, many of the Commission's proposals in this *FNPRM* will further enable wireless providers to take targeted and aggressive next steps in this ongoing fight.

The Commission's safe harbor proposal is a key part of the solution to relieve consumers from the pain of unwanted and illegal robocalls. As the Commission recognizes, a safe harbor from strict liability for voice service providers' good-faith efforts to curb abusive robocalls will

---

[4] Comments of CTIA, CG Docket No. 17-59, at 3 (Sept. 24, 2018) (citations omitted) ("In the short time since the *2017 Call Blocking Order* went into effect, AT&T reports that it 'has blocked a total of 74 telephone numbers, preventing more than 5 million illegal calls from reaching its post-paid wireless customer base, including fixed and mobile wireless customers.' This is in addition to the more than 4 billion illegal robocalls that AT&T has blocked under its program to 'identify and block illegal traffic on its wholesale network from customers of its IP-based call termination service.' T-Mobile reports that it has blocked 986 million calls in the year ending August 31, 2018.") ("*CTIA Sept. 2018 Comments*"); Letter from Kathleen O'Brien Ham, Senior Vice President, Government Affairs, T-Mobile, to Commissioner Geoffrey Starks, Federal Communications Commission, at 2 (July 10, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-358443A12.pdf ("[T-Mobile] alert[s] customers to an average of 1 billion 'Scam Likely' calls per month and as of this month, have identified 15 billion 'Scam Likely' calls. In the two years since Scam ID launched, [T-Mobile] ha[s] blocked 3.2 billion calls with Scam Block.") ("*T-Mobile Starks Letter*"). Importantly, robocall blocking volume is not a perfect metric, but it provides an indication of providers' effectiveness at stemming the tide of illegal robocalls.

[5] FCC Chairman Proposes Banning Malicious Caller ID Spoofing of Text Messages & Foreign Robocalls, FCC (July 8, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-358339A1.pdf; *see also FNPRM*, ¶ 2 (characterizing a declaratory ruling as part of the Commission's "multi-pronged strategy to curb illegal robocalls").

give them certainty and incentives to more aggressively combat unwanted and illegal robocalls.[6] A safe harbor will also help set expectations so legitimate callers can avoid being mistaken for illegal callers and inadvertently blocked. A properly tailored safe harbor will help calling parties deliver the calls consumers want and will help voice service providers meaningfully reduce the number of illegal and unwanted calls that reach consumers.

CTIA urges the Commission to adopt a safe harbor for voice service providers' call blocking efforts based on reasonable analytics, which may include SHAKEN/STIR data. A safe harbor limited to call-blocking based only on failed SHAKEN/STIR authentication protects consumers using just one arrow in the quiver. A broader, yet predictable safe harbor will empower providers to combat the challenging and evolving threat from illegal and unwanted robocalls with every innovative tool and approach available, without the need for additional Commission action.

As they fight abusive robocallers, CTIA's member companies share the Commission's focus on ensuring completion of legitimate calls, especially critical calls—consumer trust and safety depend on it. The Commission can help voice service providers meet these goals by clearly defining "critical calls" and allowing industry and public safety stakeholders to develop solutions to protect them. Increased certainty for voice service providers and legitimate callers alike, combined with flexibility to innovate, will help ensure critical calls are protected. While the Commission's proposal for a centralized "list" may be one way to protect critical calls, the Commission should consider further input from industry, public safety, calling party, and other stakeholders about the appropriate solutions to protect these calls.

[6] *See FNPRM*, ¶ 59 (noting that "adopting a safe harbor would greatly facilitate" efforts to reduce illegal and unwanted robocalls "by providing carriers with more certainty"); *see also FNPRM*, ¶¶ 24–25 (issuing the "declaratory ruling to resolve uncertainty and make clear the call-blocking tools that voice service providers can offer their customers" because other factors had "muddied the legal waters for voice service providers").

The Commission should ensure that whatever approach it chooses is flexible enough to align with actions by Congress, which is fighting alongside the Commission to combat and limit illegal and unwanted robocalls. The Commission should avoid prescriptive approaches or rules that may conflict with pending legislation or changes in the nascent robocall-blocking ecosystem. Finally, the Commission should recognize the challenges of evaluating robocall mitigation effectiveness and refrain from imposing data collection, reporting, or other requirements. The Commission should allow the wireless industry to dedicate all available resources to continue to fight illegal and unwanted robocalls on all fronts.

II. THE WIRELESS INDUSTRY IS ANSWERING THE CALL TO RELIEVE CONSUMERS FROM THE SCOURGE OF ILLEGAL AND UNWANTED ROBOCALLS.

Robocalls are a major pain point for consumers,[7] and the wireless industry is answering the call to help. Using the clear authority to implement call blocking tools provided by the Commission,[8] CTIA's member companies are implementing a variety of technologies, including network-level tools that consumers never see, as well as consumer-facing tools consumers can download and subscribe to.[9] The market for call-blocking analytics engines and applications is

[7] *Report on Robocalls*, Report, CG Docket No. 17-59, ¶¶ 9–14 (rel. Feb. 2019) ("*FCC Robocall Report*").

[8] *See, e.g., Rules and Regulations Implementing The Telephone Consumer Protection Act of 1991, et al.*, Declaratory Ruling and Order, 30 FCC Rcd 7961, ¶ 2 (July 10, 2015) ("Nothing in the Communications Act or our implementing rules prohibits carriers or Voice over Internet Protocol (VoIP) providers from implementing consumer-initiated call-blocking technology that can help consumers stop unwanted robocalls."); *FNPRM*, ¶ 2 (describing 2017 *Call Blocking Report and Order and Further Notice of Proposed Rulemaking* and actions taken in the Declaratory Ruling that are "essential to curtail illegal calls"). Still, CTIA urges the Commission to grant even broader call blocking authority to carriers. As CTIA has argued, "[t]he FCC should broadly authorize voluntary carrier-initiated blocking and not limit its authorization to calls originating from narrow categories of numbers." *CTIA Sept. 2018 Comments*, at 4.

[9] *See Commissioner Starks Releases Free Robocall Blocking Responses*, FCC (Jul. 11, 2019), https://www.fcc.gov/document/commissioner-starks-releases-free-robocall-blocking-responses; ("*July 2019 Starks Response Letters*"); *Rosenworcel Releases Responses to Call for Robocall Blocking Tools*, FCC (Jan. 28, 2019), https://www.fcc.gov/document/rosenworcel-releases-responses-call-robocall-blocking-tools ("*January 2019 Rosenworcel Response Letters*"); Comments of CTIA, WT Docket No. 17-59, at 3–4 (June 30, 2017) (describing provider efforts initiated more than two years ago) ("*CTIA June 2017 Comments*"); *see also Consumer Resources: iOS Robocall Blocking*, CTIA, https://www.ctia.org/ios-robocall-blocking (collecting current blocking resources

growing rapidly, with a variety of anti-robocall stakeholders teaming up to develop innovative consumer protection solutions.[10] These actions are making a real difference. While call volume is not a perfect metric to track the effectiveness of robocall blocking, wireless providers have already blocked *billions* of illegal robocalls.[11]

Beyond call blocking, CTIA's member companies are continuing their multi-pronged fight against illegal robocallers. For example, industry is driving the SHAKEN/STIR framework, a next-generation technological approach to improve call authentication and mitigate spoofing. The national wireless providers—who have all committed to implementing SHAKEN/STIR by the end of 2019[12]—have made significant progress toward achieving this Commission priority. For example: AT&T recently completed an authenticated call using SHAKEN/STIR between two separate networks—a key milestone to achieving widespread adoption;[13] T-Mobile launched its "Caller Verified" technology in January using SHAKEN/STIR;[14] and Verizon started using SHAKEN/STIR in March.[15] Major providers underscored their commitments to continued collaboration and progress at the Commission's July 11, 2019 summit on SHAKEN/STIR.[16]

---

from, *inter alia*, AT&T, T-Mobile, Verizon); *Consumer Resources: Android Robocall Blocking*, CTIA, https://www.ctia.org/consumer-resources/how-to-stop-robocalls/android-robocalls-blocking/ (same).

[10] *See e.g., Call Blocking: Eliminate Unwanted Callers*, YOUMAIL, https://www.youmail.com/home/feature/call-blocking ("YouMail keeps a large list of up to 500,000 generally unwanted robocallers at any one time. It also lets you add numbers to that list . . . When these numbers call, your phone won't ring, they'll hear an out of service message, and YouMail will hang up on them."); *Nomorobo*, NOMOROBO, https://nomorobo.com/ (noting that Nomorobo has stopped over 1.1 billion robocalls).

[11] *CTIA Sept. 2018 Comments*, at 3 (citations omitted); *T-Mobile Starks Letter*, at 2.

[12] *See generally July 2019 Starks Response Letters*.

[13] *AT&T, Comcast Announce Anti-Robocalling Fraud Milestone Believed to be Nation's First*, AT&T (Mar. 20, 2019), https://about.att.com/story/2019/anti_robocall.html.

[14] *T-Mobile First to Launch Caller Verification to Help Protect Consumers from Scams*, T-MOBILE (Jan. 10, 2019), https://www.t-mobile.com/news/caller-verified-note9.

[15] *Verizon offers new ways to battle robocalls*, VERIZON (Mar. 28, 2019), https://www.verizon.com/about/news/verizon-offers-new-ways-battle-robocalls.

[16] *See Chairman Pai Convenes SHAKEN/STIR Robocall Summit*, Public Notice, DA 19-413 (rel. May 13, 2019); *SHAKEN/STIR Robocall Summit*, FCC (July 11, 2019), https://www.fcc.gov/SHAKENSTIRSummit.

Industry has also led the way in traceback efforts. Using call authentication technology to identify the origin of illegal robocalling campaigns, voice service providers are promoting the ability of the Commission's Enforcement Bureau and other law enforcement entities to pursue bad actors.[17] Industry participants have come together in the USTelecom Industry Trace Back ("ITB") Group to share information to more effectively trace illegal robocalls.[18] The ITB Group is focused on improving the speed of traceback, expanding traceback capacity, and broadening information sharing. Collaborative traceback efforts are uniquely valuable because they help prevent bad actors from using providers' networks and help enforcement entities target those bad actors.[19] The Commission recognizes that "the USTelecom Industry Traceback Group has been instrumental," and "[o]ver the course of two years . . . the amount of time necessary to conduct a traceback investigation from start to finish has shrunk from months to weeks."[20]

While these efforts have gained ground against illegal and unwanted robocallers, there is still work to do. Industry has been vocal in identifying and developing more defenses against illegal and unwanted robocalls, and the Commission has made additional grants of authority and proposed a safe harbor.[21] At this critical stage in the fight against illegal and unwanted robocalls, the Commission should adopt a broad, predictable safe harbor that allows providers to use all reasonable robocall blocking tools available so that providers can unleash a full-fledged defense against abusive robocallers.

---

[17] *See The USTelecom Industry Traceback Group (ITG)*, USTELECOM (Apr. 29, 2019), https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg/; *see also FNPRM*, ¶ 55 ("The Industry Traceback Group, which is led by USTelecom, works to identify the source of illegal calls and works with law enforcement to bring the perpetrators to justice.").

[18] *CTIA Sept. 2018 Comments* at 17–18.

[19] *CTIA Sept. 2018 Comments* at 17–18.

[20] Letter from Rosemary C. Harold, Chief, Enforcement Bureau, to Jonathan Spalter, President & CEO, USTelecom – The Broadband Association (Nov. 6, 2018), *available at* https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf.

[21] *See e.g., FNPRM*, ¶ 2 (describing 2017 *Call Blocking Report and Order and Further Notice of Proposed Rulemaking* and actions taken in the Declaratory Ruling that are "essential to curtail illegal calls").

III. THE COMMISSION SHOULD ADOPT A BROAD SAFE HARBOR TO ENSURE THAT PROVIDERS CAN OFFER CONSUMERS A VARIETY OF ROBUST ROBOCALL-BLOCKING SOLUTIONS.

CTIA urges the Commission to adopt a safe harbor that protects voice service providers from liability for inadvertent blocking of legitimate calls based on *any* reasonable call-blocking analytics—which means permitting providers to rely on more than just a call's failed authentication under the SHAKEN/STIR framework. The record in this proceeding shows that "a broad safe harbor is necessary to encourage aggressive unwanted call blocking actions to protect consumers, protect voice providers from liability for inadvertently blocking legal calls, and give industry the flexibility and incentives to continuously innovate."[22] An appropriately tailored safe harbor will help achieve the Commission's dual goals of incentivizing providers to develop and use call-blocking tools and ensuring completion of legitimate calls.

The Commission was right to propose a safe harbor to enable voice service providers to deploy more aggressive protections against illegal and unwanted robocalls, and enhance legitimate callers' ability to regain consumer trust. Without a safe harbor, voice service

[22] *Ex Parte* Presentation of CTIA and USTelecom at 3 n.9, CG Docket No. 17-59, WC Docket No. 17-97 (May 30, 2019) ("*CTIA May 2019 Ex Parte*") (citing Comments of AT&T, CG Docket No. 17-59, at 11 (Sept. 24, 2018)) ("Service providers need the protection of a safe harbor to ensure continued innovation and experimentation to combat illegal robocalls."); Reply Comments of CTIA, CG Docket No. 17-59, at 5 & n.14 (Oct. 9, 2018) (explaining that there is "a clear need for safe harbors to encourage aggressive call blocking to protect consumers," including "a safe harbor for carriers that offer optional (either opt-in or opt-out) call labeling and blocking services, or that partner with third-party providers of such services for the benefit of their customers") ("*CTIA Oct. 2018 Reply Comments*"); Comments of ITTA—The Voice of America's Broadband Providers, CG Docket No. 17-59, at 4 (Sept. 24, 2018) ("As long as the provider is acting in good faith within the contours of the rules the Commission adopts, it should be immune from any Commission enforcement liability for legitimate calls blocked or illegal calls that are not blocked. So long as the provider complies with the guidelines the Commission sets forth to protect legitimate callers, a provider should not be subject to any enforcement liability where a legitimate call ends up being blocked accidentally or, conversely, where an illegitimate caller mistakenly ends up on the white list."); Comments of Transaction Network Services, CG Docket No. 17-59, at 3 (Sept. 24, 2018) ("Some operators seek more clarity on safe harbor provisions before implementing more aggressive blocking practices. Apart from this comment, TNS defers to our carrier partners with respect to any questions about whether and which additional steps may be appropriate before service providers consider blocking a call."); Comments of The USTelecom Association, CG Docket No. 17-59, at 4 (Sept. 24, 2018) ("The Commission should adopt a safe harbor to provide certainty to voice providers that choose to institute blocking measures consistent with the rules adopted in this proceeding.").

providers may face liability and unknown damages for good faith, inadvertent blocking and as a result, may be wary of pursuing all available solutions to combat and prevent abusive robocalls absent a safe harbor. But the proposed, narrow safe harbor for calls blocked based on failed Caller ID authentication under the SHAKEN/STIR framework limits voice service providers to just one line of defense. It is important to remember that SHAKEN/STIR, or any other single tool for that matter, is not a "silver bullet" and cannot alone stop the flood of illegal and unwanted robocalls.[23]

In order to meet public and policymaker expectations for meaningfully relieving the pain of abusive robocalls, voice service providers need the ability to use *any* reasonable call-blocking tools to determine whether to block an unwanted or illegal call.[24] In addition, the safe harbor should apply *generally*, meaning that it should apply to network-level blocking and consumer-facing blocking tools; it should apply equally to voice service providers of all sizes; and it should apply to all calls—regardless of whether they originate domestically or internationally. A broad and generally applicable safe harbor will achieve both of the Commission's goals of encouraging voice service providers to aggressively fight illegal and unwanted robocalls and ensuring the completion of legitimate calls.

[23] Chairman Pai on the SHAKEN/STIR Robocall Summit (July 11, 2019) *available at* https://docs.fcc.gov/public/attachments/DOC-358430A1.pdf (noting that "there is no silver bullet to solving the problem of unwanted robocalls") ("*Chairman Pai July 2019 Summit Statement*"); Comments of T-Mobile, CG Docket No. 17-59, at 4 (Sept. 24, 2018) ("SHAKEN/STIR is not a panacea, however. First, SHAKEN/STIR can only provide a positive affirmation of the source of a given call. It cannot provide confirmation of the opposite—that is, that a call is definitively 'bad' or fraudulent.") ("*T-Mobile Sept. 2018 Comments*").

[24] *FNPRM*, ¶ 35 (finding that to be "reasonable," analytics "must be applied in a non-discriminatory, competitively neutral manner.").

A. The Commission Is Right to Propose a Safe Harbor for Voice Service Providers Working to Mitigate the Scourge of Illegal and Unwanted Robocalls.

A safe harbor will serve the Commission's policy goals, which CTIA shares: to fight illegal and unwanted voice calls and to help promote legitimate call completion. *First*, a clear safe harbor will expedite progress in the fight against illegal and unwanted calls, which is "the Commission's top consumer protection priority."[25] As providers implement more call-blocking tools, the volume of blocked calls will increase, as well as the reality that some legitimate calls may be inadvertently blocked. Without a safe harbor, voice service providers may face liability for good faith, inadvertent blocking.[26] Call originators have told the Commission that "[t]he carriers are rightly concerned about their potential liability for blocking legitimate calls."[27] Accordingly, the Commission is correct that "a safe harbor would greatly facilitate [call blocking] effort[s] *by providing carriers with more certainty*."[28] Providers will be incentivized to more aggressively police illegal and unwanted robocalls if they know that their good faith efforts to defend consumers will be protected.[29]

---

[25] *FNPRM*, ¶ 1.

[26] *See e.g.,* 47 C.F.R. §§ 201, 202; 47 C.F.R. § 64.2101, *et seq.*; *see also* Comments of CTIA at 3 n.4, CG Docket No. 17-59, DA 18-638 (July 20, 2018) ("Without a safe harbor for authorized call blocking, carriers continue to face risks related to inadvertent call blocking."); *CTIA June 2017 Comments*, at 14 ("The Commission should adopt a rule stating that no complaint, cause of action, or enforcement proceeding shall be maintained under federal or state law against any provider that blocks a call under a good-faith belief that such blocking is permissible under FCC rules. . . . Without such a safe harbor, carriers could face liability for unintended and unknowable consequential damages.").

[27] *See e.g., Ex Parte* Letter of Professional Association for Customer Engagement, 2-3, CG Docket No. 17-59 (May 29, 2019).

[28] *FNPRM*, ¶ 59 (emphasis added). The Commission is correct that "the benefit to consumers of providing a safe harbor for voice service providers that block. . . will exceed any costs incurred by voice service providers." *Id.*

[29] *CTIA June 2017 Comments*, at 14; *see also FNPRM*, ¶ 2 (explaining that safe harbor for SHAKEN/STIR "will encourage the widespread deployment of the SHAKEN/STIR framework").

Second, a safe harbor will promote the completion of legitimate calls—another key priority of the Commission.[30] The safe harbor will help set expectations for legitimate calling parties so they can help ensure their calls will be completed.[31] Additionally, a robust safe harbor will encourage more call blocking, reducing the overall number of illegal and unwanted robocalls, "mak[ing] it more likely that [consumers] will answer their phones, thus making it easier for legitimate callers to reach people" and "ultimately increas[ing] call completion rates for legitimate callers."[32]

B. The Safe Harbor Should Be Broad Enough to Protect Voice Service Providers' Use of All Reasonable Call Blocking Tools.

CTIA strongly supports a safe harbor and agrees with the Commission's reasoning that voice service providers must be assured that their good faith efforts to protect consumers from illegal and unwanted robocalls fall within a safe harbor.[33] However, CTIA asks the Commission to establish a safe harbor that extends the fight against robocalls beyond just those calls that fail SHAKEN/STIR authentication, allowing providers to target any call that reasonable analytics determine to be illegal or unwanted.[34]

---

[30] *See Rural Call Completion*, Second Report and Order and Third Further Notice of Proposed Rulemaking, 33 FCC Rcd 4199, ¶ 1 (Apr. 17, 2018) ("All Americans should have confidence that when a call is made to them, they will receive it. . . . Regardless of how the caller and/or called party experiences a call completion problem, the failures have serious repercussions, imposing needless economic and personal costs, and potentially threatening public safety in local communities.").

[31] As the Commission envisions, voice service providers and their analytics company partners are already working with calling parties to resolve inadvertently blocking of legitimate calls, to the extent they occur. *See FNPRM*, ¶ 38.

[32] *FNPRM*, ¶ 38. And as the Commission rightly recognized, allowing voice service providers to use call blocking technologies will cause "unwanted calls, including illegal calls, [to] consume less of their network capacity, which can then be devoted more fully to calls and other services that consumers value." *FNPRM*, ¶ 59.

[33] *See FNPRM*, ¶ 59 ("We tentatively conclude that adopting a safe harbor would greatly facilitate [call blocking efforts] by providing carriers with more certainty.").

[34] The Commission "recognize[d] the role that analytics plays in the fight to eliminate unwanted and illegal robocalls" when it allowed voice service providers to offer call-blocking programs based on "reasonable analytics." *See FNPRM*, ¶ 62.

The Commission's proposes a "narrow" safe harbor for "voice service providers that offer call-blocking programs that take into account whether a call has been properly authenticated under the SHAKEN/STIR framework and may potentially be spoofed."[35] The Commission explains that this approach focuses only on blocking calls "that fail Caller ID authentication under the SHAKEN/STIR framework,"[36] which is just one of many inputs that may help indicate if a call is illegal or unwanted. The Commission asks whether this "strikes the appropriate balance" and whether it should "offer a more expansive safe harbor to encourage compliance or a less expansive safe harbor to account for potential technical problems."[37]

In order to properly incentivize voice service providers to offer robust call blocking, CTIA urges the Commission to adopt a broader safe harbor—based on the same "reasonable analytics" standard as is in the Opt-Out Call Blocking Declaratory Ruling ("Declaratory Ruling")—for all types of good-faith call blocking.[38] A broader safe harbor that is based on reasonable analytics, and not just one input, will strike the right balance between incentivizing voice service providers to harness all available data to uphold consumers' expectations about blocking illegal and unwanted calls, while protecting them from potential liability for inadvertently blocking legitimate calls.

---

[35] *FNPRM*, ¶ 49. The Commission clarifies that "a call is authenticated when the terminating provider checks the attestation information against the originating or gateway provider's certificate," which occurs only after the call is signed, or attested, by the originating provider or gateway provider, by inserting the header described in the SHAKEN/STIR standards. *See id.* ¶ 50.

[36] *FNPRM*, ¶ 51.

[37] *FNPRM*, ¶ 53. The Commission also asks whether it should "create a safe harbor for blocking unsigned calls from particular categories of voice service providers." *Id.*, ¶ 54.

[38] *See FNPRM*, ¶ 34 (recognizing that limiting "call-blocking programs to rigid blocking rules that prescribe in detail when a voice service provider may block is unnecessary" and "could enable callers to evade blocking, and could impede the ability of voice service provider to develop dynamic blocking schemes that evolve with calling patterns"); *id.*, ¶ 35 (noting, in addition to SHAKEN/STIR, "several examples of call-blocking programs that may be effective and would be based on reasonable analytics designed to identify unwanted calls"); *id.*, ¶ 35 (finding that to be "reasonable," analytics "must be applied in a non-discriminatory, competitively neutral manner").

1. The Safe Harbor Should Allow Voice Service Providers to Block Calls Based on All Reasonable Analytics, Which May Include SHAKEN/STIR Data.

The Commission should establish a safe harbor that encourages call blocking based on any reasonable analytics.[39] The wireless industry fully supports SHAKEN/STIR and believes SHAKEN/STIR implementation will significantly improve voice service providers' ability to authenticate calls.[40] But SHAKEN/STIR is not the only way, or the best way, to determine whether calls should be blocked.[41] SHAKEN/STIR was designed to authenticate the originating

---

[39] As the Commission recognized, call-blocking programs based on reasonable analytics may be effective and may block large bursts of calls in a short timeframe, calls with low average duration, or calls that analytics indicate are illegal or unwanted based on other factors. *See FNPRM*, ¶ 35. Voice service providers and their analytics company partners echo the Commission's view, and offer solutions that rely on a wide variety of data and sophisticated analytics to determine that a call is likely fraudulent. *See, e.g.*, Comments of First Orion Corp., CG Docket No. 17-59, at 3-4 (July 20, 2018); Testimony of Scott Hambuchen, Executive Vice President, Technology Solution and Development, First Orion Corp. before the House Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection, at 11 (Apr. 27, 2018); Verizon Comments, CG Docket No. 17-59, at 12 (July 20, 2018).

[40] *See, e.g.*, Letter from Joan Marsh, Executive Vice President, Regulatory & State External Affairs, AT&T, to Commissioner Geoffrey Starks, Federal Communications Commission, at 1–2 (July 10, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-358443A2.pdf ("AT&T also is a leader in the deployment of the SHAKEN/STIR protocols. AT&T helped to develop the standards, played an active role on the NANC working group that established the governance framework for industry implementation, currently chairs the Governance Authority Board that recently selected the SHAKEN Policy Administrator, and is deploying the standards in its network this year—ahead of broader industry implementation and consistent with Chairman Pai's stated expectations."); *T-Mobile Starks Letter*, at 2 ("In addition to developing its own suite of consumer tools, T-Mobile was the first carrier to announce readiness for the FCC-recommended STIR/SHAKEN standards in November 2018 and first to implement "Caller Verified" in January 2019 on its network. We were also first in the industry to launch STIR/SHAKEN across networks with Comcast Xfinity in April 2019. We now have Caller Verified on 10+ devices with more to come in 2019."); Letter from Charles W. McKee, Vice President Government Affairs Federal and State Regulatory, Sprint, to Commissioner Geoffrey Starks, Federal Communications Commission, at 1 (July 10, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-358443A10.pdf ("Sprint was part of the FCC's North American Number Council's Call Authentication Trust Anchor Working Group that led to the establishment of SHAKEN/STIR Governance Authority. As noted in Sprint's November 19, 2018, letter to Chairman Pai, Sprint is fully committed to the implementation of SHAKEN/STIR by the end of 2019.") ("*Sprint Starks Letter*"); Letter from Kathleen Grillo, Senior Vice President, Verizon, to Commissioner Geoffrey Starks, Federal Communications Commission, at 2 (July 10, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-358443A14.pdf ("Because restoring trust in Caller ID is crucial for the overall mission of restoring trust in voice calls, Verizon is a leader in deploying STIR/SHAKEN. . . . Not only is Verizon expending substantial resources to implement STIR/SHAKEN in our own networks, but we are supporting efforts to help the entire industry adopt STIR/SHAKEN. For example, Chris Oatway on my team is on the board of the industry-led governance authority that is establishing a system for issuing to service providers the certificates needed to efficiently send and receive STIR/SHAKEN-enabled calls.").

[41] *See Chairman Pai July 2019 Summit Statement* (noting that "there is no silver bullet to solving the problem of unwanted robocalls"); *see also CTIA Oct. 2018 Reply Comments*, at 8–9 ("SHAKEN/STIR is a call authentication tool that can be used to assist in certain call blocking efforts, but should not be used as a substitute for other forms of

provider of a call, but SHAKEN/STIR does not determine the intent of the call, whether a call is legal or illegal, or whether a call is wanted or unwanted.[42] As Verizon explained, voice service providers "should complement STIR/SHAKEN with other techniques for addressing the spoofing problem."[43] Likewise, T-Mobile said its analytics provider "is critical to its ability to identify and block fraudulent traffic."[44] The Commission should not exclude from the safe harbor tools that providers deem vital to reducing the amount of fraudulent voice traffic sent to consumers.[45] Now is the time to seize all available opportunities to more aggressively stymie illegal robocallers. To allow voice service providers to take a multi-pronged approach, the Commission should adopt a robust safe harbor based on voice service providers' use of reasonable analytics.

The Commission's reasoning for adopting the reasonableness standard in the Declaratory Ruling supports adoption of CTIA's proposed broader safe harbor. There, the Commission approved of "call-blocking programs based on any reasonable analytics designed to identify unwanted calls."[46] The Commission highlighted the primary advantage of this approach:

---

call blocking. As CTIA has emphasized, the Commission, like carriers, needs to take a multi-pronged approach to fighting illegal robocalls."); *Sprint Starks Letter*, at 2 ("Sprint remains concerned that the lack of a safe harbor for accidental or erroneous call blocking could result in significant liability exposure for carriers. The proposed safe harbor for SHAKEN/STIR does not address this issue because SHAKEN/STIR data will likely be only one factor of many in deciding whether a given call is illegal or unwanted.").

[42] *See* Letter from Rebekah Johnson, CEO, Numeracle, Inc., to Marlene H. Dortch, Secretary, Federal Communications Commission, at 2 (May 30, 2019), *available at* https://prodnet.www.neca.org/publicationsdocs/wwpdf/53019num.pdf ("STIR/SHAKEN was designed to provide consistent traceback to determine the originating carrier, but STIR/SHAKEN does not determine whether a call is legal or illegal or wanted or unwanted."); *see also* 2019 Robocall Investigation Report, Transaction Network Services, at 27, *available at* https://ecfsapi.fcc.gov/file/10515248878426/Transaction%20Network%20Services%20-2019%20Robocall%20Investigation%20Report.pdf ("STIR/SHAKEN can attest to the authentication of the calling party telephone number but is not able to address the question of intent.") ("*2019 TNS Robocall Report*").

[43] Comments of Verizon, CG Docket 17-59, at 6 (July 20, 2018).

[44] *T-Mobile Sept. 2018 Comments*, at 4-5.

[45] *See T-Mobile Sept. 2018 Comments*, at 5 ("As the work continues toward the IP transition and initiatives such as SHAKEN/STIR, the Commission should be careful not to prohibit use of these types of tools that T-Mobile believes are important to its efforts to reduce the amount of fraudulent traffic sent to its end users.").

[46] *FNPRM*, ¶ 34. While the Commission referenced opt-out call-blocking programs in the Declaratory Ruling, CTIA's proposed safe harbor would protect calls blocked based on voice service providers use of reasonable

flexibility for voice service providers to take steps to end illegal and unwanted voice calls.[47] The Commission explained that "rigid call blocking rules . . . could enable callers to evade blocking, and could impede the ability of voice service providers to develop dynamic blocking schemes that evolve with calling patterns."[48]

The Commission was right. A narrow safe harbor based only on failed SHAKEN/STIR authentication is the type of rigid rule that will hinder providers' efforts to block illegal and unwanted calls and enable bad actors to evade detection.[49] On the other hand, a robust safe harbor based on reasonable analytics will give voice service providers flexibility "to develop dynamic blocking schemes that evolve with calling patterns."[50]

A safe harbor should also apply generally, to protect both network-level blocking and consumer-facing blocking tools.[51] Today, voice service providers use many tools to protect consumers.[52] Network-level call-blocking tools are implemented by voice service providers to improve consumers' service seamlessly.[53] Consumer-facing tools, such as call-blocking apps, are offered by providers on an opt-in or opt-out basis to empower consumers to protect themselves from illegal and unwanted calls.[54] Network-level and consumer-facing tools are distinct in that they apply call blocking techniques at different stages in transmission,[55] but both

analytics via either network-level, opt-out call-blocking programs or consumer-facing opt-in or opt-out call-blocking programs.

[47] *FNPRM*, ¶ 34.

[48] *FNPRM*, ¶ 34.

[49] *See 2019 TNS Robocall Report*, at 27 ("Bad actors will be able to make malicious calls from numbers that they have been assigned by a provider, and will be able to burn through those numbers, then move on to the use of new numbers to avoid detection.").

[50] *FNPRM*, ¶ 34.

[51] *CTIA May 2019 Ex Parte* at 3.

[52] *See, e.g., January 2019 Rosenworcel Response Letters*; *July 2019 Starks Response Letters.*

[53] *See FNPRM*, ¶ 23 (noting that "network-based blocking" is "blocking without consumer choice").

[54] *CTIA May 2019 Ex Parte*, at 3.

[55] *CTIA May 2019 Ex Parte*, at 3.

network-level, provider-initiated blocking and consumer-facing blocking tools are crucial to the fight against robocalls.[56] The safe harbor should include both of these blocking tools.

The Commission should also consider including in the safe harbor voice service providers who participate in, and cooperate with, industry-led traceback and call authentication efforts. As discussed, collaborative industry traceback efforts are valuable to providers and enforcement entities in targeting bad actors.[57] The Commission should promote these efforts by treating participation in traceback as an indicator that a provider is working in good faith to help identify bad actors.

Finally, the safe harbor should apply equally to voice service providers of all sizes, and to calls that originate domestically or from a foreign country. Illegal and unwanted robocalls may originate from, or be facilitated by, small or large providers located in America or abroad.[58] The Commission should encourage voice service providers to leverage Caller ID authentication, including SHAKEN/STIR, to combat illegal calls no matter where they originate. The safe harbor should not provide a carve-out for certain categories of voice service providers.

2. At a Minimum, the Commission Should Broaden the Safe Harbor to Cover Calls Blocked Based on Various Levels of SHAKEN/STIR Attestation.

While CTIA urges the Commission, as described above, to adopt a broad safe harbor for calls blocked based on reasonable analytics, at a minimum, the Commission should broaden the proposed safe harbor to cover calls blocked based on varying degrees of SHAKEN/STIR

[56] *See CTIA May 2019 Ex Parte*, at 3; *see also T-Mobile Starks Letter*, at 1 ("[N]etwork solutions provide real-time decisions on incoming calls, intelligent analysis of phone call and network-wide data, and an adaptable machine-learning based framework to stop the next scammer tactic.").
[57] *See* Section II, *supra*.
[58] *FNPRM*, ¶ 82 ("Illegal robocalling often originates from sources outside the United States.").

attestation.[59] Whether a call has failed SHAKEN/STIR authentication alone is not dispositive of whether the call is illegal or illegitimate. Some legitimate calls may fail SHAKEN/STIR authentication through no fault of the originating or terminating provider. For example, a dropped header or protocol conversion error could lead to authentication failure.[60] Conversely, bad actors may develop techniques that allow illegal and unwanted calls to pass SHAKEN/STIR authentication.[61] The safe harbor should account for these situations by covering the use of reasonable analytics, but at a minimum, the safe harbor should cover calls blocked based on varying degrees SHAKEN/STIR attestation.

Using all SHAKEN/STIR data—including whether a call receives partial or gateway attestation, as opposed to simply whether it fails authentication—provides a voice service provider with more data to inform reasonable call-blocking decisions. Providers should be encouraged to use all available data and analytics related to SHAKEN/STIR, including partial attestations, to develop robust and "dynamic blocking schemes that evolve with calling patterns."[62] With a broader safe harbor, providers will be able to leverage the SHAKEN/STIR framework to its full potential,[63] which will go further in helping stop illegal and unwanted robocalls.[64]

---

[59] Additional scenarios described by the Commission, such as "call-blocking programs that consider the degree of attestation (whether full, partial or gateway)" should fall within a safe harbor. *FNPRM*, ¶ 53.
[60] A safe harbor that considers varying degrees of SHAKEN/STIR attestation would help "account for potential technical problems" like these. *See FNPRM*, ¶ 53.
[61] *See e.g., Certificate Management for STIR/SHAKEN*, TRANSNEXUS (2019), https://transnexus.com/whitepapers/stir-shaken-cms-solutions/ (white paper explaining how failure to secure private data keys could undermine SHAKEN/STIR).
[62] *FNPRM*, ¶ 34; *see also CTIA June 2017 Comments*, at 17 ("Flexibility is an essential tool in the fight against illegal robocalls.").
[63] The Commission asks: "How can we best promote the use of SHAKEN/STIR-based analytics to fight the scourge of illegal robocalls?" and "What steps should we take to encourage or require the use of SHAKEN/STIR-based analytics?" *FNPRM*, ¶ 62. Including the use of full SHAKEN/STIR data under safe harbor protections will appropriately encourage implementation and use of SHAKEN/STIR-based analytics.
[64] *See FNPRM*, ¶ 34 ("As USTelecom states in arguing for flexibility, 'a diversity of approaches would create a more challenging operating environment for illegal robocallers.'" (citation omitted)).

C. A Broader Safe Harbor Will Promote Industry Efforts to Ensure Completion of Legitimate Calls.

CTIA's members are focused on ensuring their customers receive legitimate calls and are developing improved tools to prevent false positives. CTIA shares the Commission's goals of "address[ing] false positives," and "ensur[ing] that wanted calls are not blocked."[65] However, CTIA does not support proposals to restrict the safe harbor or require providers to implement specific "mechanisms" to ensure completion of wanted calls.[66] The Commission should encourage industry efforts to address these issues by adopting the broad safe harbor described above and avoiding prescriptive mandates or technical requirements for multiple reasons.

Voice service providers share the Commission's prioritization of call completion because they have every incentive to deliver legitimate calls.[67] Accordingly, industry takes concerns about overblocking and false positives seriously and is working to mitigate the inadvertent blocking of legitimate calls.[68] As the use of call-blocking tools increases, some false positives will inevitably occur even with providers' good-faith efforts to focus only on bad actors. Voice service providers engaged in call blocking have mechanisms in place to minimize and remedy false positives, such as robust due diligence procedures to verify the legitimacy of calls and mechanisms for calling parties to report inadvertently blocked calls. For example, AT&T has "established procedures designed to ensure no legitimate traffic is impacted by its illegal robocall blocking program," such as "regularly refresh[ing] its list of blocked telephone numbers to

---

[65] *See FNPRM*, ¶¶ 52, 58.
[66] *See FNPRM*, ¶ 58 (asking whether "there are any particular protections we should establish for a safe harbor to ensure that wanted calls are not blocked" including "require[ing] voice service providers seeking a safe harbor to provide a mechanism for identifying and remedying the blocking of wanted calls," "to send an intercept message," or other approaches).
[67] *CTIA Sept. 2018 Comments*, at 19; *see also CTIA Oct. 2018 Reply Comments*, at 10–13 ("[C]arriers and third-party service providers are focused on preventing false positives, as has been made clear in this docket.").
[68] *CTIA Sept. 2018 Comments*, at 19–20.

ensure that stale blocks are removed in a timely manner, thus avoiding adverse impacts on consumers."[69]

Stakeholders throughout the robocall ecosystem—voice service providers, call originators, vendors, and analytics companies—are collaborating to ensure completion of legitimate calls. For example, AT&T provides a link on its website "that allows call originators to contact AT&T about" inadvertent blocking concerns and has worked with the Professional Association for Customer Engagement "to develop best practices for call originators to avoid mislabeling or, worse, the inadvertent blocking of a legitimate call."[70] A variety of identity verification tools and other call authentication solutions are developing. T-Mobile, for example, offers the Name ID application for customers who want to directly mange categories of robocalls to help ensure wanted calls, such as appointment reminders, are not blocked.[71] The Commission should encourage these evolving, cooperative solutions rather than adopting prescriptive regulations. Allowing industry to come together and innovate will promote exactly the multi-pronged anti-robocall attack the Commission has been calling for.

IV. CRITICAL CALLS SHOULD BE PROTECTED AND THE COMMISSION SHOULD WORK WITH INDUSTRY AND PUBLIC SAFETY STAKEHOLDERS TO PROVIDE GUIDANCE.

CTIA shares the Commission's objective to protect critical calls. The Commission can help voice service providers meet this goal by defining "critical calls" and allowing industry and public safety stakeholders to develop solutions to protect them. Increased certainty about what a critical call is, combined with flexibility to innovate, will help ensure critical calls are protected.

---

[69] Comments of AT&T at 8, 11, CG Docket No. 17-59 (July 20, 2018) ("*AT&T July 2018 Comments*").
[70] *AT&T July 2018 Comments*, at 8.
[71] *See What is T-Mobile Name ID?*, T-MOBILE, https://www.t-mobile.com/resources/name-id ("Name ID includes advanced features such as personal number blocking, reverse number lookup and the ability to send entire categories of callers-such as telemarketers and political surveyors, directly to voicemail.").

A. CTIA's Member Companies Take Seriously Their Roles in Completing Emergency and Critical Calls.

Voice service providers are focused on ensuring the completion of emergency and critical calls.[72] CTIA's members know that consumers depend on a reliable communications system, especially in emergencies, to deliver critical calls.[73] Because of the vast range of sources and types of calls that could be considered critical, voice service providers engage in substantial due diligence and leverage all available data to protect these calls. As voice service providers are working hard to protect critical calls, CTIA and its member companies welcome guidance from the Commission on how best to do so.

B. The Commission Should Define Critical Calls and Promote Development of Industry Solutions.

The Commission correctly recognizes that providers should avoid blocking certain calls and proposes requiring voice service providers that engage in call blocking to maintain a "Critical Calls List." CTIA agrees that protecting critical calls must be a priority for voice service providers, especially as they more aggressively deploy call-blocking tools based upon reasonable analytics. The Commission should work with CTIA's member companies and other stakeholders, primarily the public safety community, to define "critical calls" and seek further input on whether a centralized Critical Calls List is the best approach to protecting critical calls.

---

[72] Voice service providers are heavily engaged in the Commission's public safety efforts. They are active in the recent emergency call proceeding, regarding implementation of Kari's Law and Section 506 of RAY BAUM's Act. Numerous working groups of the Communications Security, Reliability, and Interoperability Council work on public safety issues, and CTIA's members work with NENA: The 9-1-1 Association regularly. Voice service providers are—and will remain—committed to ensuring the completion of emergency calls.

[73] *See e.g.,* Aaron C. Davis and Sandhya Somashekhar, *The Only California County That Sent A Warning To Residents' Cellphones Has No Reported Fatalities*, WASH. POST (Oct. 13, 2017), https://www.washingtonpost.com/investigations/the-only-california-county-that-sent-a-warning-to-residents-cellphones-has-no-reported-fatalities/2017/10/13/b28b5af4-b01f-11e7-a908-a3470754bbb9_story.html?utm_term=.48ba09096409 (explaining how reverse 911 calls can save lives).

1. The Commission Should Define Critical Calls To Promote Certainty.

While voice service providers are doing everything they can to protect critical calls, they seek guidance from the Commission on the meaning of "critical call" to improve their approaches. Given that the meaning of "critical call" is unclear,[74] the Commission should clarify that the term "critical call" includes "genuine emergency calls"[75] and calls from public safety entities, and also whether it includes calls that "consumers value,"[76] and/or other types of calls the Commission describes. Defining a "critical call" will be challenging, but it is necessary. It is unlikely that any one metric—such as call volume, calling entity, call source—will be determinative of whether a call is "critical." Further, consumers and calling parties may have varying views of what should be considered a "critical call." The Commission should be mindful of these complexities while striving toward a definition that will give providers certainty and help protect critical calls.

Increased certainty about what a *bona fide* emergency call or other critical call is will enable voice service providers, public safety entities, and other stakeholders in the call-blocking and authentication space to adopt consistent approaches to protecting critical calls. Commission guidance will also help establish consumer expectations about what calls are "critical."[77] While Commission guidance on the definition of a "critical calls" will help achieve the Commission's goals, prescriptive rules or technical requirements will not. The Commission should give voice

[74] Commission starts from the premise that "[c]ertain *emergency* calls must never be blocked," but then creates the potential for confusion by asking whether to include other calls that "are *important* to consumers." *See FNPRM*, ¶¶ 63, 66 (emphasis added).
[75] *FNPRM*, ¶ 64 (internal quotations omitted).
[76] *FNPRM*, ¶ 66.
[77] For example, the Commission's conception of a "critical call" appears to be based on the identity of the caller, not necessarily the content of the call. Accordingly, while a consumer might consider a call from their child's school to alert them of an emergency to be a critical call, the narrower list proposed by the FCC—limited to 911 call centers and government emergency outbound numbers—would not capture that expectation.

service providers and other robocall ecosystem stakeholders' flexibility to use Commission guidance to develop solutions to protect critical calls.

2. A Centralized Critical Calls List Involves Complex Choices and the Commission Should Ensure that the Approach It Takes Promotes Continued Innovation from Industry.

The Commission seeks comment on whether to develop a centralized Critical Calls List. Such a list, whether managed by the FCC or other entity, may be one approach that helps protect critical calls. However, developing such a centralized list raises complex issues. The Commission should solicit specific industry feedback on any solution it pursues.

The security of any centralized list or other solution is of utmost importance. A Critical Calls List would present a target for bad actors. As the FTC has cautioned, a centralized list poses a risk that illegal and unwanted robocallers will obtain numbers on the list and spoof critical calls.[78] A Critical Calls List would need to be kept confidential to prevent spoofing, as the Commission anticipates,[79] but that raises questions about how a list (or lists) would be maintained, who would have access, and what criteria would govern how entities would qualify to be included on the Critical Calls List. Promoting the security of any list should be a top priority.

Defining the scope of the Critical Calls List will also be important but challenging. An overbroad Critical Calls List may risk becoming an overbroad whitelist if it includes all calls that "consumers value."[80] Such a list could also increase the volume of illegal or unwanted robocalls

[78] *FNPRM*, ¶ 64 & n.111.
[79] *FNPRM*, ¶ 68.
[80] *Cf. FNPRM*, ¶ 64 ("[A] limited list is also likely easier to define and more manageable than opening it up to a broader set of callers."). Indeed, the American Dental Association has already recommended "that the primary phone number of dental offices be provided to voice service providers for inclusion in [any FCC] white list" because its "member dentists feel strongly that calls from dental offices to their patients, including automated calls and voice messages, promote oral health, for example, by reminding the patients to schedule a needed teeth cleaning or other service." *See* Comments of the American Dental Association, CG Docket No. 17-59 (July 10, 2019).

that reach consumers by inadvertently including spoofed critical caller phone numbers.[81] While too narrow a list may not include all numbers related to critical calls, a more targeted list will prevent abuse, pose a lower risk of including spoofed numbers, and will better protect consumers from illegal and unwanted robocalls.

The Commission should seek input from the public safety community, voice service providers, and other robocall ecosystem stakeholders to develop its approach to critical calls—whether by developing a Critical Calls List or other solutions. The Commission should also consider industry solutions that help identify and authenticate call originators and other privately developed options to protect critical calls. Any approach the Commission takes should promote continued innovation and collaboration to protect emergency and other critical calls.

V. THE COMMISSION SHOULD ENSURE ITS ROBOCALL MITIGATION EFFORTS ARE FLEXIBLE ENOUGH TO ALIGN WITH CONGRESSIONAL ACTIONS AND MARKETPLACE DEVELOPMENTS.

CTIA commends the hard work of both the Commission and Congress in combating the scourge of illegal and unwanted robocalls. While Congress considers legislation and the robocall blocking marketplace evolves, the Commission should ensure that its approach can be compatible with future Congressional action and account for changing robocaller tactics and call-blocking approaches.

Like the Commission, Congress has heard consumers' calls for help in fighting illegal and unwanted robocalls. Pending legislation, like the TRACED Act[82] and the Stopping Bad Robocalls Act ("SBRA"),[83] offers a step forward. Both bills are largely consistent with the

[81] *See FNPRM*, ¶ 64 ("[T]he Federal Trade Commission cautions that a centralized white list mechanism creates a risk that illegal callers will obtain those numbers and spoof them in order to reach consumers.").
[82] Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S. 151, 116th Cong. ("TRACED Act").
[83] Stopping Bad Robocalls Act, H.R. 3375, 116th Cong. ("SBRA").

Commission's proposals. They reflect a growing consensus to promote implementation of the SHAKEN/STIR framework but recognize that providers need more tools to protect consumers,[84] and the TRACED Act includes a robust safe harbor.[85] The legislation would also empower the Commission to help stop illegal robocalls at their source and encourages a "whole of government" approach to illegal and unwanted robocalls at the federal and state levels.[86]

Until Congress acts, the Commission should take an approach that is flexible enough to align with the legislation Congress may pass. This will avoid potentially inconsistent requirements. Ensuring that voice service providers, analytics companies, and other stakeholders understand Congress' and the Commission's expectations will help promote call authentication implementation and prevent potential future inconsistency and uncertainty.

The Commission should also preserve flexibility for voice service providers, equipment manufacturers, and application developers to innovate in response to consumer demand and changing illegal robocaller tactics. As noted above, the national wireless providers—who have all committed to implementing the SHAKEN/STIR framework by the end of 2019[87]—have already made significant progress toward achieving this Commission priority. Companies are also developing different displays and tools to communicate call authentication to consumers, including those based on SHAKEN/STIR.[88] The anti-robocall marketplace is still developing,

---

[84] *See* Kelly Cole & Matthew Gerst, *Taking a Bite Out of Unwanted Robocalls*, CTIA (May 30, 2019), https://www.ctia.org/news/taking-a-bite-out-of-unwanted-robocalls.
[85] TRACED Act, § 3(c)(1)(B),
[86] *See* Kelly Cole & Matthew Gerst, *Taking a Bite Out of Unwanted Robocalls*, CTIA (May 30, 2019), https://www.ctia.org/news/taking-a-bite-out-of-unwanted-robocalls.
[87] *See generally July 2019 Starks Response Letters*.
[88] Voice service providers are focused on ensuring the effectiveness of authentication displays, and are developing offerings that take into account challenges posed by visual displays. For instance, web page security experts have increasingly abandoned early visual cues, citing consumer confusion and icon mimicking by fraudulent phishing sites and lack of customer attention to persistent, positive indicators versus rare, negative indicators. *See, e.g.*, Adrienne Porter Felt, Robert W. Reeder, et al., *Rethinking Connection Security Indicators*, Proceedings of the Twelfth Symposium on Usable Privacy and Security 2016, Denver, CO, June 22-24, 2-7; Lily Hay

and prescriptive rules will only hinder the pace of progress. The Commission should encourage continued innovation and should not restrict providers' flexibility to experiment with the SHAKEN/STIR framework and other tools to "enhance the consumer experience."[89]

VI. MONITORING ROBOCALL BLOCKING EFFORTS CAN PROMOTE PROGRESS, BUT MEASURING EFFECTIVENESS IS COMPLEX.

CTIA supports the Commission's goal to use robocall mitigation data to inform its policy.[90] Data on robocall mitigation efforts can provide the Commission and industry with insight on the state of the marketplace and the effectiveness of tools. Voice service providers are using various data analytics tools to identify unwanted calls,[91] and are measuring their call traffic and call-blocking efforts in diverse ways. As a result, measuring the effectiveness of robocall blocking efforts is complex. The Commission should continue to monitor the progress of work to block illegal and unwanted robocalls but should not impose burdensome data collection or reporting requirements on voice service providers.

The robocall mitigation market is still in its nascent stages, and stakeholders are developing a variety of solutions to block illegal and unwanted robocalls and a variety of metrics to track these efforts.[92] Accordingly, measuring effectiveness is difficult because these

---

Newman, *Phishing Scams Are Using Encrypted Sites to Seem Legit*, Wired, Dec.5, 2017; Alfred Ng, *Google Chrome Says Goodbye to Green 'Secure' Lock on HTTPS Sites*, CNet, May 18, 2018.

[89] *FNPRM*, ¶ 74. "Enhancing the consumer experience" is a broad concept, that includes direct enhancements through consumer-facing authentication displays, but also network improvements, including enhanced call-blocking ability, that are not visible to the consumer.

[90] The Commission plans to collect data on the deployment of Caller ID authentication through implementation of the SHAKEN/STIR framework, the availability of call blocking tools, "the number of illegal robocalls transiting our phone system," and "metrics pertaining to the use of each type of call blocking service," among other relevant data points. *FNPRM*, ¶ 90.

[91] *See CTIA Sept. 2018 Comments*, at 16 ("Data analytics providers are developing an array of analytics tools that help subscribing carriers and customers to identify calls that are likely to be illegal.").

[92] *See e.g., Consumer Resources: How to Stop Robocalls*, CTIA, https://www.ctia.org/consumer-resources/how-to-stop-robocalls (noting triple digit growth in call blocking apps over a period of less than two years). And as CTIA has explained, the future of robocall blocking will include a broad mix of tools. *CTIA May 2019 Ex Parte* at 4.

approaches are not readily amenable to a uniform metric.[93] Despite providers' best efforts, many of the existing and most intuitive metrics are subject to significant limitations:

- Call Volume: While call volume is an important metric, it is not tracked consistently across organizations.[94] Moreover, call volume does not provide information about the content of calls—*e.g.*, good or bad; wanted or unwanted.[95]

- Call Completion Rates: Even when a call blocking or labeling tool has worked properly, letting a legitimate call through, the consumer often ignores the call—this makes call completion data imperfect.

- Consumer Survey Data: While survey data may be helpful, it is costly to obtain and little currently exists.

Making robocall metrics publicly available may also prove difficult. Given the above limitations, this information may be misleading or confusing if presented to consumers. It may also discourage providers from pursuing innovative, new call blocking solutions that may perform well on some metrics but not on others. Finally, some public disclosures could provide insights to bad actors, who may use information to engineer around providers' mitigation techniques.

Despite these limitations, mitigation effectiveness information is valuable and can ultimately help both industry and the Commission make better, more informed choices. Consequently, CTIA urges the Commission to refrain from adopting burdensome reporting and/or public disclosure requirements but supports the Commission's efforts to monitor and ensure the continued progress of robocall mitigation.

[93] The Commission itself asks how to define the "effectiveness" of robocall blocking solutions. *FNPRM*, ¶ 83.
[94] *FCC Robocall Report*, ¶ 7 ("The data generally combine all types of robocalls—illegal and legal, unwanted and wanted. Further complicating any analysis is that various entities track information differently, yielding results that are not directly comparable.").
[95] *See id.*

VII. CONCLUSION

CTIA is grateful for the Commission's dedication to combating illegal and unwanted robocalls. The wireless industry is committed to regaining consumer trust in voice service, and stopping abusive robocallers is key to this end. CTIA urges the Commission to adopt a broad, predictable safe harbor to empower voice service providers to launch a stronger defense against illegal and unwanted robocalls. With this safe harbor, guidance from the Commission on protecting critical calls, and flexibility to develop new anti-robocaller solutions, CTIA's member companies will march towards their common goal of ending the scourge of robocalls for Amercian consumers.

Respectfully submitted,

/s/ Sarah Leggin

Sarah Leggin
Director, Regulatory Affairs

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Matthew Gerst
Vice President, Regulatory Affairs

CTIA
1400 16th Street, NW
Suite 600
Washington, DC 20036
(202) 736-3200
www.ctia.org

July 24, 2019