

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

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

REPLY 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 of Regulatory Affairs

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

August 23, 2019

TABLE OF CONTENTS

I.	THE RECORD CONFIRMS THAT A BROAD SAFE HARBOR IS NECESSARY TO ENABLE VOICE SERVICE PROVIDERS TO MORE AGGRESSIVELY PROTECT CONSUMERS FROM ILLEGAL AND UNWANTED ROBOCALLS.....	2
II.	THE WIRELESS INDUSTRY IS COMMITTED TO THE COMPLETION OF LEGITIMATE, WANTED, AND CRITICAL CALLS.	5
A.	Providers Need Flexibility to Respond to Consumer Feedback About Completing Legitimate Calls.	5
B.	The Record Confirms that Critical Calls Need To Be Protected and the Commission Should Work with Stakeholders to Determine the Right Approach. .	8
III.	THE COMMISSION’S <i>OPT-OUT DECLARATORY RULING</i> IS CRUCIAL TO THE FIGHT AGAINST ILLEGAL AND UNWANTED ROBOCALLS.....	10
IV.	CONCLUSION	11

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

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

REPLY COMMENTS OF CTIA

CTIA respectfully submits these reply comments in response to the Federal Communications Commission’s (“FCC” or “Commission”) Further Notice of Proposed Rulemaking (“FNPRM”) on additional steps to encourage robocall-blocking services.¹ As the record shows, voice service providers are working hard to relieve consumers from the pain of unwanted and illegal robocalls.² Commenters agree that a broad safe harbor is necessary to encourage more aggressive efforts. In addition, the record demonstrates voice service providers’ commitment to completing legitimate and critical calls, and supports a flexible approach to protect these calls that includes collaboration among industry and public safety stakeholders. Finally, the record makes clear that the Commission should reject calls to roll back the recent *Opt-Out Declaratory Ruling*, which will be a crucial tool in the fight against robocalls.

¹ *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”).

² See e.g., Comments of AT&T, CG Docket No. 17-59, at 2 (filed July 24, 2019) (“AT&T Comments”) (showing that AT&T has blocked or labeled more than seven billion suspected fraud or spam calls); Letter from Charles W. McKee, Vice President, Government Affairs, Sprint, to Geoffrey Starks, Commissioner, FCC, at 1 (July 10, 2019) (Sprint, in partnership with Transaction Network Services “has processed hundreds of millions of calls for millions of Sprint customers and has categorized 222 million calls as being nuisance or malicious, thereby enabling Sprint’s customers to block or decline to answer these calls.”); T-Mobile Comments at 3–5 (explaining that T-Mobile alerts customers to nearly a quarter billion “Scam Likely” calls per week); Letter from Kathleen Grillo, Senior Vice President, Public Policy & Government Affairs, Verizon, to Geoffrey Starks, Commissioner, FCC, at 1 (July 10, 2019) (explaining how recent incorporation of SHAKEN/STIR into analytics allows it “to make better decisions about whether to block or label a call as spam.”).

I. THE RECORD CONFIRMS THAT A BROAD SAFE HARBOR IS NECESSARY TO ENABLE VOICE SERVICE PROVIDERS TO MORE AGGRESSIVELY PROTECT CONSUMERS FROM ILLEGAL AND UNWANTED ROBOCALLS.

Stakeholders across the voice service ecosystem are calling on the Commission to encourage the use of all reasonable tools and analytics, including SHAKEN/STIR data, to inform call blocking decisions.³ The record makes clear that, consistent with CTIA’s proposal,⁴ the Commission should adopt a robust safe harbor that protects voice service providers’ call blocking decisions based on reasonable analytics, beyond the safe harbor the Commission proposed that is limited to call blocking based only upon SHAKEN/STIR data.

The record confirms that voice service providers, including CTIA’s member companies, are leading the development, governance, and deployment of SHAKEN/STIR —an important tool that will help regain consumer trust in caller-identification information.⁵ However, the record also makes clear that whether a call is verified or unverified through SHAKEN/STIR may not be a sufficient, or even necessary, basis to determine whether to block an illegal or unwanted call.⁶ That is because a failed SHAKEN/STIR attestation may not paint a complete picture, and analytics are necessary to determine whether to block a call. As Sprint points out, calls that fail

³ See, e.g., AT&T Comments at 12–13; Comments of T-Mobile USA, Inc., CG Docket No. 17-59, at 5–9 (filed July 24, 2019) (“T-Mobile Comments”); Verizon Comments on Further Notice, CG Docket No. 17-59, at 11-12 (filed July 24, 2019) (“Verizon Comments”); Comments of Sprint Corporation, CG Docket No. 17-59, at 2–4 (filed July 24, 2019) (“Sprint Comments”); Comments of First Orion Corp., CG Docket No. 17-59, at 14 (filed July 24, 2019) (“First Orion Comments”); Comments of Numeracle, Inc., CG Docket No. 17-59, at 3 (filed July 24, 2019) (“Numeracle Comments”); Comments of USTelecom – The Broadband Association, CG Docket No. 17-59, at 7–9 (filed July 24, 2019) (“USTelecom Comments”).

⁴ See CTIA Comments, CG Docket No. 17-59, at 7-18 (filed July 24, 2019) (“CTIA Comments”).

⁵ See AT&T Comments at 4–5 (explaining that AT&T co-authored SHAKEN/STIR standards and chairs oversight); T-Mobile Comments at 2 (noting T-Mobile was “the first wireless provider to implement STIR/SHAKEN standards on its network in November 2018”); Verizon Starks Letter at 2 (“Not only is Verizon expending substantial resources to implement STIR/SHAKEN . . . , but we are supporting efforts to help the entire industry adopt STIR/SHAKEN.”); Sprint Comments at 6 (“Sprint . . . supports universal adoption of SHAKEN/STIR by all voice providers.”).

⁶ See, e.g., AT&T Comments at 6 (“[T]he presence or absence of SHAKEN/STIR verification *on its own* is neither necessary nor sufficient to indicate that a call should be blocked today. . . In short, more is needed than SHAKEN/STIR information to enable a provider to determine whether a call should be blocked.”).

SHAKEN/STIR authentication “[will] likely . . . be a small subset of the total volume of illegal and unwanted calls.”⁷ For example, calls that have a full SHAKEN/STIR attestation may be unwanted or illegal, such as when a bad actor has used a SHAKEN/STIR-verified number to make an illegal robocall.⁸ In those cases too, analytics and other tools are crucial in determining the content and intent of the call, and helping the provider decide whether to block it.⁹ Given these realities, voice service providers should be incented to block calls based on more than just SHAKEN/STIR data.

Voice service providers block calls for the sole purpose of relieving consumers from the scourge of illegal and unwanted robocalls; they should not face liability for inadvertently blocking legitimate calls, despite their good faith efforts. The record supports adopting a safe harbor that encourages providers to use any reasonable analytics to determine whether to block a call, which may include SHAKEN/STIR data.¹⁰ Without a broader safe harbor, T-Mobile explains that “providers both large and small likely will be hesitant to block calls by default due to concerns about liability stemming from their common carrier obligation to complete calls.”¹¹ Verizon agrees that a safe harbor beyond just SHAKEN/STIR will “incentiviz[e] service providers to protect consumers with increasingly robust blocking solutions” by “giving providers a green light to block more aggressively.”¹² By assuring providers they will not face liability for

⁷ Sprint Comments at 2.

⁸ Some legitimate calls may also fail SHAKEN/STIR authentication through no fault of the originating or terminating provider due to a dropped header or protocol conversion error, for example. *See* CTIA Comments at 16.

⁹ *See* Scott Hambuchen, Chief Information Officer, First Orion, Statement at the July 11 Summit, at 2:03:15-2:03:32 (July 11, 2019) (“[D]eploying a STIR/SHAKEN solution without any analytic solution behind it . . . can be dangerous.”).

¹⁰ *See, e.g.*, AT&T Comments at 6, 10 (seeking a safe harbor that “protects providers from liability even when, despite reasonable best efforts, they inadvertently block legal calls.”); T-Mobile Comments at 8–9; Sprint Comments at 2; Comments of ACA Connects, CG Docket No. 17-59, at 7 (filed July 24, 2019); First Orion Comments at 10.

¹¹ *See* T-Mobile Comments at 2.

¹² *See* Verizon Comments at 11-12.

inadvertently blocking legitimate calls as long as they use reasonable analytics, the Commission will enable voice service providers to mount a stronger defense against illegal and unwanted robocalls.

The record also shows that expanding the safe harbor to cover call blocking based on reasonable analytics would be consistent with the Commission’s reasoning in the *Opt-Out Declaratory Ruling*. Specifically, T-Mobile and other commenters highlight parallels between the Commission’s “reasonable analytics” standard in the *Opt-Out Declaratory Ruling* and the need for a flexible safe harbor based on reasonable analytics in this item.¹³ For example, Sprint states that “[t]he Commission recognized the need for reasonable analytics in the *Declaratory Ruling* and should provide carriers with sufficient liability protection to incentivize the deployment of these additional protections.”¹⁴ And AT&T explains, “analytics are crucial to any safe harbor framework because, unlike the SHAKEN/STIR standards, analytics are specifically designed for making judgments regarding the likely content of a call and thus whether the call should be blocked.”¹⁵ Voice service providers and other stakeholders agree that providers need this flexibility to aggressively fight robocalls and are working on authentication solutions.¹⁶

For these reasons, the Commission should reject calls to adopt a narrow safe harbor or prescriptive rules about how voice service providers should use analytics. For example, Numeracle proposes a “requirement for companies seeking a safe harbor to use vetted caller information.”¹⁷ There is an emerging market for promising analytics tools that can add further

¹³ See T-Mobile Comments at 8; First Orion Comments at 13; *cf.* n.3, *supra*, showing broad record support for safe harbor to cover “reasonable analytics.”

¹⁴ Sprint Comments at 2.

¹⁵ AT&T Comments at 9.

¹⁶ See, e.g., AT&T Comments at 11–15; T-Mobile Comments at 8–9; Verizon Comments at 11–12; Sprint Comments at 2–4; Comments of Comcast Corporation, CG Docket No. 17-59, at 7–8 (filed July 24, 2019) (“Comcast Comments”); First Orion Comments at 11–12; USTelecom Comments at 7–9.

¹⁷ See Letter from Rebekah Johnson, CEO, Numeracle, Inc., to Marlene H. Dortch, Secretary, FCC, at 2 (filed Aug. 1, 2019) (stating that Numeracle strongly believes its registry should be used by all carriers).

certainty to the identity of the caller in order to minimize over-blocking legitimate calls,¹⁸ but no single tool should be required. The Commission should not try to pick winners (or losers) in the nascent robocall mitigation solution marketplace. Numeracle itself recognizes the benefits of flexibility, noting that “[t]here will be instances where carriers *need the flexibility* to block SHAKEN/STIR verified calls where reasonable analytics has identified fraudulent activity.”¹⁹ Thus, voice service providers should be empowered to use any reasonable analytics tools, directly or in partnership with third parties, to target illegal and unwanted calls and protect legitimate traffic from inadvertent blocking.

II. THE WIRELESS INDUSTRY IS COMMITTED TO THE COMPLETION OF LEGITIMATE, WANTED, AND CRITICAL CALLS.

A. Providers Need Flexibility to Respond to Consumer Feedback About Completing Legitimate Calls.

CTIA’s member companies share the Commission’s dual priorities: blocking illegal and unwanted traffic and completing legitimate traffic. Voice service providers and their analytics company partners have been monitoring and nimbly addressing call blocking practices that could inadvertently impact legitimate traffic.²⁰ For example, providers have established points of contact—email, phone, and web portal—to address inadvertent false positives:²¹

- **AT&T:** AT&T has a phone number—800-337-5373 (prompt 1)—which parties can call if they believe a call has been wrongfully blocked. It also maintains an email for the same purpose: dl-GFMOBusinessFra@att.com. Hiya, AT&T’s analytics partner, also maintains a web form for reporting issues: <https://www.att.com/reviewmycalllabel> or <https://hiyahelp.zendesk.com/hc/en-us/requests/new>.

¹⁸ *Id.* at 2 (describing how the benefits of and need for its vetted caller information tool).

¹⁹ Numeracle Comments at 4 (emphasis added).

²⁰ CTIA Comments at 17–18.

²¹ CTIA agrees that “a reasonable call-blocking program instituted by default would include a point of contact for legitimate callers to report what they believe to be erroneous blocking as well as a mechanism for such complaints to be resolved.” *FNPRM*, ¶ 38.

See, e.g., T-Mobile Comments at 9 (“The marketplace is in the best position to determine if providers are excessively blocking wanted calls, and the response to that blocking.”); CTIA Comments at 17–18.

- **Sprint:** Sprint has customer service contact—888-211-4727—where trained personnel can address concerns about legitimate calls being inadvertently blocked. Sprint also allows customers to register their phone numbers through Sprint’s analytics partner, TNS, and can contact TNS with robocall-related issues: <https://reportarobocall.com/trf/>.
- **T-Mobile:** T-Mobile has webpages for reporting suspected scam numbers or false positives: <https://www.t-mobile.com/callreporting> (for consumers) and <https://calltransparency.com> (for businesses).²²
- **U.S. Cellular:** U.S. Cellular offers a robocall information and resources webpage, which offers consumers an interactive chat feature for resolving questions: <https://www.uscellular.com/support/robocall/index.html>.
- **Verizon:** Verizon has a portal (available at www.Voicespamfeedback.com and www.spamalerts.verizon.com) that invites both legitimate calling parties and consumers to tell Verizon about calls that they believe are incorrectly blocked or labeled—both calls incorrectly identified as spam and ones that should have been identified as spam but were not. It also permits calling parties to describe their operations (such as the numbers they use and the nature of their calling campaigns), even if they are not aware of any issues with Verizon’s labeling or blocking, so that the third-party vendor that analyzes traffic for Verizon’s blocking/labeling tools can take that information into account.²³

Voice service providers and others in the ecosystem also employ processes that balance blocking unwanted and illegal calls and preventing false positives. For example, Inteliquent offers a webpage for consumers to report harassing, abusive, or fraudulent calls from Inteliquent-owned telephone numbers; the complaints that Inteliquent receives are forwarded to dedicated customer service personnel for investigation and resolution.²⁴ Bandwidth also offers a webpage with information about how Bandwidth combats illegal robocalls, which gives customers the ability to

²² Additionally, T-Mobile’s Call Protection page includes a full list of Frequently Asked Questions on Scam ID, Scam Block, Name ID, STIR SHAKEN & Caller Verified. See *Scam ID & Scam Block*, T-MOBILE (last accessed Aug. 15, 2019), <https://support.t-mobile.com/docs/DOC-38784>.

²³ Verizon also educates calling parties about the sorts of calling activities that can result in their calls being identified as spam, so that they have the opportunity to adjust their operations in order to avoid becoming caught up in Verizon’s or other parties’ blocking or labeling tools. Those educational materials are available at <https://www.voicespamfeedback.com/vsf/bestPractices>.

²⁴ See *Report Abuse*, INTELIGENT (last accessed Aug. 15, 2019), <https://www.inteliquent.com/contact-legal/report-abuse>.

chat with a representative and report spam calls.²⁵ Other consumer-facing blocking and labeling tools provide consumers with a range of information about blocked calls. For example, providers track and keep records of each customers' call history, which may include inbound illegal, invalid, or spam calls. Customers can access their call logs at their request to review their call history and provide feedback to their providers on whether the right calls are being blocked.

Given the readily accessible resources and personnel that providers and other stakeholders already make available to consumers, mandating specific solutions, as call originators and others propose, is unnecessary and potentially harmful. For example, several commenters urge the Commission to require providers to use standardized notification procedures, such as SIP code intercept messages, to inform callers when their calls have been blocked.²⁶ As a general matter, requiring all providers to use uniform solutions will actually tip off bad actors that their methods are not working, and encourage them to mount new points of attack to circumvent call blocking tools. What's more, forcing providers to alter or rebuild their solutions will drain resources and increase the burden on those trying in earnest to fight illegal robocallers. The Commission should allow providers to offer a variety of solutions, and continue to innovate and adapt their tools as the problem demands.²⁷

²⁵ See *How Bandwidth Combats Illegal Robocalls, Scam Calls, Toll Fraud, and SPAM*, BANDWIDTH, (last accessed Aug. 19, 2019), <https://www.bandwidth.com/blog/how-bandwidth-combats-illegal-robocalls-scam-calls-toll-fraud-and-spam/>.

²⁶ See, e.g., Comments of ACA International, CG Docket No. 17-59, at 11 (filed July 24, 2019) ("ACA International Comments"); Comments of Consumer Bankers Association, CG Docket No. 17-59, at 3 (filed July 24, 2019); Comments of Professional Credit Service, CG Docket No. 17-59, at 2 (filed July 24, 2019); see also Comments of INCOMPAS, CG Docket No. 17-59, at 8 (filed July 24, 2019) ("INCOMPAS Comments") (calling for "readily discoverable challenge mechanism as well as an expedited complaint or appeals process that would ensure that remedies are in place for cases of 'false positives.'"); Comments of PRA Group, Inc., CG Docket No. 17-59, at 3 (filed July 24, 2019) ("PRA Group Comments") ("We also urge the Commission to require, as a condition of any safe harbor, that Voice Service Providers implement a mechanism to notify callers and call recipients of blocked calls, and remove erroneous blocks within 24 hours.").

²⁷ For example, if there is a need to notify calling parties that their traffic is being blocked, providers should be able to provide notifications using a variety of means, including response codes or recorded messages, as appropriate. There is no need to mandate specific processes for false positives, including complaint resolution processes or blocking notification requirements. See T-Mobile Comments at 9 ("The marketplace is in the best position to

B. The Record Confirms that Critical Calls Need To Be Protected and the Commission Should Work with Stakeholders to Determine the Right Approach.

Commenters resoundingly agree that protecting critical calls is crucial.²⁸ They also agree that the issue is complex and requires further input from all stakeholders, including voice service providers, consumers, and the public safety community.²⁹

No matter what the Commission ultimately deems to be the best path forward to protect critical calls, the record supports a targeted, narrow definition of “critical call.”³⁰ A broad definition risks creating a nationwide whitelist that may prove difficult to protect and impossible to administer.³¹ Numeracle seems to suggest that a critical calls list should include *all* legal

determine if providers are excessively blocking wanted calls, and the response to that blocking.”); *see also* CTIA Comments at 17–18.

²⁸ *See, e.g.*, CTIA Comments at 18–19; Sprint Comments at 4; T-Mobile Comments at 9; Verizon Comments at 12; AARP Comments at 12 (“Calls placed to 911 must go through in all cases.”); Comments of Boulder Regional Emergency Telephone Service Authority, CG Docket No. 17-59, at 4–8 (filed July 24, 2019); Electronic Transactions Association Comments, CG Docket No. 17-59, at 2 (filed July 24, 2019); First Orion Comments at 11; Larimer Emergency Telephone Authority Comments, CG Docket No. 17-59, at 2 (filed July 23, 2019); Comments of the Massachusetts Department of Telecommunications and Cable, CG Docket No. 17-59, at 7 (filed July 24, 2019) (“MDTC Comments”); Comments of NCTA – The Internet & Television Association, CG Docket No. 17-59, at 10 (filed July 24, 2019); PRA Group Comments at 2; Comments of Securus Technologies, Inc., CG Docket No. 17-59, at 6 (filed July 24, 2019); Comments of the Voice on the Net Coalition, CG Docket No. 17-59, at 3 (filed July 24, 2019).

²⁹ *See, e.g.*, Comments of Ring Central, Inc., CG Docket No. 17-59, at 7 (filed July 24, 2019) (“[T]he idea of a Critical Calls List, as proposed, raises numerous practical challenges.”); USTelecom Comments at 9 (“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”); T-Mobile Comments at 9–10 (“[T]he question of what constitutes ‘critical calls’ and how they are identified is one that should be decided by the Commission with input from all industry stakeholders, including voice providers and the public safety community.”); Comment of Professional Association for Customer Engagement, CG Docket No. 17-59, at 6–7 (filed July 24, 2019) (“The Commission should carefully consider the ramifications of a Critical Call List.”).

³⁰ *See* CTIA Comments at 21 (“An overbroad Critical Calls List may risk becoming an overbroad whitelist if it includes all calls that consumers value.” (citation and quotation omitted)); T-Mobile Comments at 10 (“Expanding the category of critical calls beyond PSAPs will present definitional challenges that will make not blocking problematic, unwieldy, and subjective.”); Comcast Comments at 12–13 (supporting tiered approach that starts with a core definition that includes only emergency numbers).

³¹ *See, e.g.*, AARP Comments at 11 (“While it is essential that emergency calls are not blocked, the creation of a universal white list introduces a significant security problem, as is indicated by the . . . *FNPRM*.”); Sprint Comments at 5 (“Regardless of how the critical calls list is established and maintained, it should not be a white list—at least for the time being.”); CTIA Comments at 21 (“An overbroad Critical Calls List may risk becoming an overbroad whitelist if it includes all calls that consumers value.” (citation and quotation omitted)).

calls.³² Likewise, credit unions propose including a range of notifications on a critical calls list.³³ These and other proposals will be complex and unmanageable. As T-Mobile explains, a broad definition of “critical call” “will present definitional challenges that will make not blocking problematic, unwieldy, and subjective.”³⁴ The Commission should focus on genuine emergency calls. For example, calls from PSAPs are an appropriate starting point because “they represent a known and verifiable category of entities for which no blocking may be reasonably implemented.”³⁵ And commenters strongly agree that 911 callbacks and calls related to safety are effectively always “critical.”³⁶

Many commenters urge caution regarding the Commission’s proposal to develop and manage a centralized critical calls list. For example, AARP says that “[w]hile it is essential that emergency calls are not blocked, the creation of a universal white list introduces a significant security problem” and that “AARP believes, along with Consumers Union et al., that universal white lists should not be implemented until caller ID authentication has been fully implemented, including calls originating overseas.”³⁷ Other commenters suggest alternative approaches that may prove overly burdensome. For example, the Massachusetts Department of Telecommunications and Cable proposes a patchwork approach in which “state commissions” will “review any . . . lists of ‘critical calls’” to ensure “such lists are complete and adequately represent the interest of their constituencies.”³⁸ Accordingly, the record precludes concrete

³² See Numeracle Comments at 2.

³³ See, e.g., Comments of Credit Union National Association, CG Docket No. 17-59, at 6–7 (filed July 24, 2019); Heartland Credit Union Association Comments, CG Docket No. 17-59 (filed July 24, 2019) (“The list should include numbers from which the following categories of calls are initiated: fraud alerts, data breach notifications, remediation messages, utility outage notifications, product recall notices, prescription notices, and mortgage servicing calls required by Federal or State law.”).

³⁴ T-Mobile Comments at 10.

³⁵ See T-Mobile Comments at 10.

³⁶ See, e.g., Sprint Comments at 4; Twilio Comments at 3; Comcast Comments at 12.

³⁷ AARP Comments at 11-12.

³⁸ See MDTC Comments at 7–8.

action at this time. The Commission should leverage the knowledge and experience of the many engaged commenters in this proceeding to more fully consider how to protect critical calls.

III. THE COMMISSION’S *OPT-OUT DECLARATORY RULING* IS CRUCIAL TO THE FIGHT AGAINST ILLEGAL AND UNWANTED ROBOCALLS.

The Commission should reject suggestions to rescind any part of the *Opt-Out Declaratory Ruling*, even as SHAKEN/STIR becomes widely deployed. The Commission’s June 2019 *Opt-Out Declaratory Ruling* gives voice service providers the necessary flexibility to rely on “reasonable analytics” to block calls on an opt-out basis.³⁹ Commenters are grateful to the Commission for giving voice service providers the clear authority to use this important tool.⁴⁰ Indeed, they hailed the *Declaratory Ruling* as “a major milestone in the fight against illegal and unwanted robocalls.”⁴¹

Rescinding providers’ ability to offer call blocking and labeling tools based on reasonable analytics would be a retreat in the battle against illegal and unwanted robocalls. The commenters arguing to the contrary cannot justify their proposals. They posit that following SHAKEN/STIR implementation, “the Commission should rescind the portion of the *Declaratory Ruling* allowing voice service providers to rely on ‘reasonable analytics’ to block calls on an opt-out basis.”⁴²

³⁹ See *FNPRM*, ¶¶ 34-35.

⁴⁰ See, e.g., CTIA Comments at 13–14 (endorsing Commission’s flexible “reasonable analytics” standard); AT&T Comments at 2; T-Mobile Comments at 1; Verizon Comments at 1; First Orion Comments at 10 (explaining the superiority of a “holistic approach” allowing “reasonable analytics”); Comcast Comments at 2 (“The ... *Declaratory Ruling* allowing for broader use of certain blocking techniques, coupled with a Third Further Notice of Proposed Rulemaking (‘Third *FNPRM*’) ... represents another laudable step forward.”).

⁴¹ See, e.g., AT&T Comments at 2; Verizon Comments at 1 (“The Commission’s declaratory orders authorizing more extensive robocall blocking are important and laudable steps forward in the war on robocalls.”).

⁴² ACA International Comments at 8-9 (arguing that full deployment of SHAKEN/STIR “will obviate the need to use ‘reasonable analytics’ to determine whether a ‘robocall’ is ‘unwanted.’”); see also Comments of the American Association of Healthcare Administrative Management (“AAHAM”), CG Docket No. 17-59, at 4 (filed July 24, 2019) (“[T]he Commission should clarify that the permissibility of opt-out blocking based on ‘reasonable analytics’ is provisional, pending completion of SHAKEN/STIR.”) (“AAHAM Comments”); Comments of TCN Inc., CG Docket No. 17-59, at 5–6 (filed July 24, 2019) (“[I]f [formal SHAKEN/STIR] rules are adopted, the Commission should withdraw the *Declaratory Ruling*’s discussion on allowing voice service providers to block ‘unwanted’ calls on an opt-out basis.”).

Roll-back proposals misunderstand the utility of SHAKEN/STIR. As noted above, SHAKEN/STIR is not intended to identify whether a call is illegal or unwanted; it is intended to authenticate caller ID.⁴³ While the roll-back proponents claim that limiting blocking to calls that fail SHAKEN/STIR authentication will result in fewer false positives, the record suggests the opposite. As explained above, legitimate calls may fail SHAKEN/STIR authentication⁴⁴ so providers need flexibility to use additional data and tools to determine whether to block a call. Restricting reasonable analytics to include only SHAKEN/STIR inputs will still result in inadvertent blocking of legitimate calls, and will also deprive providers of full access to the plethora of reasonable call blocking tools available.

As the record proves, voice providers need the ability to use a broad range of tools to fight illegal and unwanted robocalls. The *Declaratory Ruling* provides clear authority for providers to use one set of tools.⁴⁵ While industry continues to make strides, the effectiveness of various defenses against bad robocalls is not clear and will likely evolve over time. The Commission should not take away any consumer protection tools.

IV. CONCLUSION

CTIA's member companies will continue to support and work with the Commission to achieve their shared goal to end harmful robocalls. At the same time, the Commission can help ensure the completion of legitimate and critical calls by clearly defining critical calls and allowing industry flexibility to protect them. And by adopting a broader safe harbor based on

⁴³ Letter from Rebekah Johnson, CEO, Numeracle, Inc., to Marlene H. Dortch, Secretary, FCC, at 2 (May 30, 2019).

⁴⁴ See *supra* Section I; CTIA Comments at 16.

⁴⁵ See Section II.A. AAHAM cites CTIA's comments on last year's robocall mitigation public notice for the proposition that SHAKEN/STIR is an "accurate technical solution to malicious calls from bad actors." AAHAM Comments at 3 n.5. This misunderstands CTIA's comments. As CTIA explained, call authentication is one tool in an evolving ecosystem of solutions. Comments of CTIA, CG Docket No. 17-59, at 11 (filed July 20, 2018) ("many efforts remain in their early stages. Ecosystem participants are evaluating the effectiveness of tools, and it is too soon to know how various efforts will impact illegal robocalling. . . . Call authentication, discussed above, is *one such tool*." (emphasis added)).

reasonable analytics and upholding the robocall blocking authority provided in the *Declaratory Ruling*, the Commission will strengthen industry's efforts to protect customers from the plague of illegal and unwanted robocalls.

Respectfully submitted,

/s/ Sarah Leggin

Sarah Leggin
Director of 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

August 23, 2019