Before the
Federal Communications Commission
Washington, D.C.

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	WC Docket No. 17-59
	)	
	)	

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 K. Leggin
Director, Regulatory Affairs

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

August 31, 2020

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY. 1

II. ADDITIONAL SAFE HARBOR PROTECTIONS CAN ENHANCE VOICE SERVICE PROVIDERS' ABILITY TO PROTECT CONSUMERS FROM UNWANTED AND ILLEGAL ROBOCALLS. 4

A. The Commission's Call-Blocking Safe Harbors Are Critical to Voice Service Providers' Aggressive Efforts to Protect Consumers From Unwanted and Illegal Robocalls. 5

B. The Commission's Proposed Safe Harbor for Network-Level Blocking Can Further Enhance Consumer Protections and Incent Voice Service Providers' Robocall Mitigation Strategies. 7

C. The Commission Should Consider Additional Safe Harbors to Further Empower and Protect Consumers as Robocall Mitigation Tools Develop. 11

III. AS VOICE SERVICE PROVIDERS WORK TO COMPLETE LEGITIMATE CALLS, THE COMMISSION SHOULD CONTINUE TO PROMOTE FLEXIBILITY IN ROBOCALL MITIGATION AND BLOCKING REDRESS PROGRAMS. 13

A. Any Commission Action Related to Providers' Unique Robocall Mitigation Programs Should Promote Adaptability and Innovation. 14

B. The Commission Should Encourage Innovative Labeling Tools that Empower Consumers and Promote Flexible Redress Options for Legitimate Calling Parties to Work with Voice Providers to Resolve Reports of Erroneous Call Blocking. 16

IV. CONCLUSION. 19

Before the
Federal Communications Commission
Washington, D.C.

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	WC Docket No. 17-59
	)	
	)	

COMMENTS OF CTIA

CTIA[1] respectfully submits these comments on the Federal Communications Commission's ("FCC" or "Commission") *Fourth Further Notice of Proposed Rulemaking* ("*FNPRM*"), which accompanies its *Third Report and Order* ("*Order*") establishing call-blocking safe harbors and seeking input on additional steps to further protect consumers from unwanted and illegal robocalls, as well as continue implementation of the TRACED Act.[2] CTIA and its member companies throughout the wireless industry support the Commission's ongoing efforts to ensure that voice service providers have sufficient protections for call-blocking decisions made to protect consumers from illegal and unwanted robocalls, while also encouraging reasonable efforts to protect legitimate callers.

I. INTRODUCTION AND SUMMARY.

Protecting consumers from unwanted and illegal robocalls continues to be one of the

[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*, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, WC Docket No. 17-59 (July 17, 2020) ("*Order and FNPRM*" or "*Order"* or "*FNPRM"*); Pallone-Thune TRACED Act, S. 151, 116th Cong. (2019) ("*TRACED Act*").

Commission's top priorities,[3] and CTIA and its member companies agree that "with the collective efforts of government and industry, we are making progress."[4] CTIA's member companies are hard at work implementing or offering new services and solutions to protect consumers from illegal and unwanted robocalls, while proceeding cautiously to protect legitimate calls. As the Commission described in its recent *Report on Call Blocking*, wireless voice service providers are leading the way in deploying call-authentication technology based on STIR/SHAKEN, developing and deploying robust call-blocking programs, and participating with industry partners in tracebacks to stop bad actors at the source, among other initiatives.[5] In these comments, CTIA encourages the Commission to adopt its proposed network-level blocking safe harbor that can further protect voice service providers who block calls that are highly likely to be illegal before they reach consumers, while maintaining sufficient flexibility for providers to deploy innovative anti-robocall solutions and protect legitimate callers.

CTIA commends the Commission's many efforts that empower voice service providers to protect consumers from unwanted and illegal robocalls.[6] Specifically, the Commission's

---

[3] *Order and FNPRM* ¶ 1.

[4] *Order and FNPRM,* Statement of Chairman Pai. As the FCC concluded in its June 2020 Report on Call Blocking, industry has "taken strong action to provide tools for consumers to block unwanted and illegal calls." *Call Blocking Tools Now Substantially Available to Consumers: Report on Call Blocking,* CG Docket No. 17-79, A Report of the Consumer and Governmental Affairs Bureau, Federal Communications Commission, 36 (June 2020) ("*Report on Call Blocking*"). Wireless providers report blocking more than one million illegal robocalls every day. *See* CTIA Consumer Resources—How to Stop Robocalls, https://www.ctia.org/consumer-resources/how-to-stoprobocalls (last visited June 9, 2020).

[5] *See Report on Call Blocking*, at 7-8 (June 2020) ("*Report on Call Blocking*"). *See also, e.g.*, *T-Mobile Unveils Latest Un-carrier Move: Scam Shield – A Massive Set of Free Solutions to Protect Consumers from Rampant Scams and Robocalls*, T-Mobile Blog (July 16, 2020), https://www.t-mobile.com/news/un-carrier/scam-shield-protects-customers-from-scams-robocalls (offering free services consumers can turn on to label or block scam calls, provide enhanced caller ID service, or change phone numbers if a personal phone number becomes a spam target) ("*T-Mobile Scam Block Announcement.*").

[6] *See, e.g.*, Patrick Webre, *Building on the Promise of Call Blocking*, FCC Blog (July 9, 2020), https://www.fcc.gov/news-events/blog/2020/07/09/building-promise-call-blocking ("*Building on the Promise of Call Blocking Blog*").

recent adoption of a broad and flexible safe harbor for call blocking harnessing reasonable analytics based on consumer-facing tools,[7] and a safe harbor targeting illegal traffic from bad-actors[8] will empower voice service providers to more confidently deploy robust blocking tools and protocols without fear of liability for their good faith efforts to protect consumers.

In addition to these two safe harbors, CTIA urges the Commission to adopt the proposed network-level blocking safe harbor[9] and consider additional safe harbors—such as for trust identification, as contemplated in the TRACED Act—to encourage the development of additional robocall mitigation tools.[10] A network-level call-blocking safe harbor that mitigates providers' liability for actions to block calls that are highly likely to be illegal before they reach consumers can encourage voice service providers to take even stronger actions to protect consumers from robocalls and fight bad actors in the highly dynamic and evolving robocall environment.[11]

---

[7] *Order* ¶ 25 ("[W]e adopt a safe harbor from liability under the Communications Act and the Commission's rules for the unintended or inadvertent blocking of wanted calls where terminating voice service providers block based on reasonable analytics that include caller ID authentication information and the consumer is given the opportunity to opt out.").

[8] *Id.* ¶ 36 ("We clarify that voice service providers may block calls from certain bad-actor upstream voice service providers and we establish a safe harbor from liability related to call completion obligations arising under the Communications Act and the Commission's rules for this blocking.").

[9] *See FNPRM* ¶¶ 104-06. Network-level or network-based blocking is done by providers on behalf of their customers without those customers having to opt in or out, is specifically designed to block calls that are highly likely to be illegal, and is managed with sufficient human oversight and network monitoring to ensure that blocking is working as intended. *See id.*; *see also infra* at 7-8.

[10] *See FNPRM* ¶ 87. TRACED Act § 4(c)(1)(B) (directing the Commission no later than one year after enactment of the TRACED Act to, "establish[] a safe harbor for a provider of voice service from liability for unintended or inadvertent blocking of calls or for the unintended or inadvertent misidentification of the level of trust for individual calls based, in whole or in part, on information provided by the call authentication frameworks."). *See also SHAKEN 101: Mitigating Illegal Robocalling and Caller ID Scams Webinar*, ATIS (Jan. 30, 2019), https://www.atis.org/wp-content/uploads/01_news_events/webinar-pptslides/SHAKEN101_%20MitigatingIllegalRobocalling01302019.pdf (describing trust levels or "attestation levels" used to indicate various levels of call verification—full, partial, or gateway attestation—within the SHAKEN protocol).

[11] *See e.g.*, Comments of Verizon, CG Docket No. 17-59, at 5-6 (filed July 20, 2018) ("Bad Actors Evolve Their Techniques to Bypass Blocking and Filtering Tools."); 2020 Robocall Investigation Report, Transaction Network

While voice service providers are committed to stopping bad robocalls, providers are also taking steps to help ensure that legitimate calls are delivered. For example, providers have already deployed a variety of tools and services to mitigate unwanted robocalls and provide redress for reports by legitimate callers of erroneous call-blocking. CTIA encourages the Commission to continue a reasonable, flexible approach to enhance anti-robocall solutions, as well as any redress solutions. A flexible approach is the best way to support voice service providers' ongoing efforts to do even more to protect consumers from unwanted and illegal robocalls.

II. ADDITIONAL SAFE HARBOR PROTECTIONS CAN ENHANCE VOICE SERVICE PROVIDERS' ABILITY TO PROTECT CONSUMERS FROM UNWANTED AND ILLEGAL ROBOCALLS.

CTIA commends the Commission's many efforts that are empowering the wireless industry to answer the call to help protect consumers from unwanted and illegal robocalls.[12] The two safe harbors established by the Commission will enhance consumer protections by ensuring that providers can confidently address unwanted and illegal robocalls using all of the tools available to them. By adopting the proposed safe harbor to further encourage network-level blocking of calls that are highly likely to be illegal, as well as additional safe harbors, such as for trust identification, as contemplated in the TRACED Act, the Commission can encourage voice service providers to deploy and evolve their robocall mitigation solutions to protect consumers.

Services, at 18 (March 2020), *available at* https://tnsi.com/forms/tns-robocall-report-mar-2020/ ("The one constant in the robocall dilemma is that bad actors change tactics quickly.") ("*2020 TNS Report*").

[12] *See, e.g.*, *Building on the Promise of Call Blocking Blog* ("For some time now, stopping unwanted and illegal calls has been the FCC's top consumer protection priority. In addition to aggressive enforcement activity and consumer education, we have focused on creating an effective regulatory environment that enables and encourages phone companies and others to proactively stop unwanted robocalls from ever reaching customers."); Comments of CTIA, CG Docket No. 17-59, WC Docket No. 17-97, at 4, 6 (Jan. 29, 2020) ("[T]he wireless industry and its robocall mitigation partners have protected consumers from *tens of billions* of illegal and unwanted robocalls.").

A. The Commission's Call-Blocking Safe Harbors Are Critical to Voice Service Providers' Aggressive Efforts to Protect Consumers From Unwanted and Illegal Robocalls.

The Commission is right to remove regulatory uncertainty by adopting safe harbors for certain call blocking by voice service providers[13] that will help encourage and empower providers to take further action to protect consumers from illegal and unwanted calls. By adopting a safe harbor that protects providers' good-faith efforts to block calls based on reasonable analytics, the Commission has enhanced voice service providers' ability to use all information available to inform call treatment decisions in a highly dynamic and evolving robocall landscape.[14] The Commission was also right to decline a narrower approach to these safe harbors that would have only protected providers' call-blocking actions taken in reliance on STIR/SHAKEN attestation alone, which the record made clear is not enough to inform a call treatment decision, particularly given the evolving techniques employed by illegal robocallers.[15] By promoting providers' use of sophisticated analytics and caller ID authentication information where available,[16] the adopted safe harbor promotes a more holistic and flexible decision-making

[13] *See Order* ¶ 22.

[14] *See id.* ¶¶ 25-34.

[15] *See id.* ¶ 48 (declining to adopt "both safe harbors [the Commission] proposed that took into account only STIR/SHAKEN caller ID authentication information without incorporating other reasonable analytics"). As various stakeholders have explained, call-blocking decisions take into account a variety of data and sophisticated analytics to help determine whether to block a call, which may include STIR/SHAKEN, but that standard is not determinative of a call-blocking decision. As the *Order* correctly notes, the STIR/SHAKEN standards are neither "an ubiquitous or a comprehensive indicator of whether a consumer should answer a call," nor were the standards "designed to distinguish wanted and unwanted calls." *See id.* ¶ 29.

[16] *See e.g.*, Reply Comments of Hiya, WC Docket Nos. 17-97, 20-67, at 4-6 (May 29, 2020) (stating that "while the attestation level is an important new signal that will provide great benefit to call originators and consumers alike by restoring trust in the phone call, the attestation level is by no means the only—or most important—signal used in determining the caller reputation."); Letter from Jennifer Glasgow, EVP, Policy and Compliance, First Orion Corp., to Ms. Marlene H. Dortch, Secretary, FCC, at 2 (July 9, 2020) (stating that it is "widely acknowledged—including in the STIR/SHAKEN standards work—that analytics are required to determine the intent of callers. Reasonable analytics IS the investigation into the call and is far more effective than placing calls and trying to ascertain the intent of calling parties.") (emphasis in original).

framework that voice service providers can "adapt to evolving threats"[17] when protecting consumers from illegal and unwanted robocalls.

CTIA also supports the Commission's adoption of a safe harbor that targets bad-actors, which will help incentivize providers to more aggressively police their networks by shielding providers that work to effectively mitigate bad traffic that pass through critical points within the voice telephone system.[18] Given that "specific providers can pass large volumes of bad traffic,"[19] the Commission is right that encouraging providers and their partners to attack the problem closer to its source will increase the effectiveness of providers' blocking efforts.[20] This safe harbor will also promote providers' ability to protect a broad range of consumers, regardless of a consumers' network capabilities. By encouraging providers to block all traffic from a given bad-actor provider, this safe harbor helps protect consumers in cases where the consumer may not have activated opt-in mitigation tools, where network technology may not support call authentication tools—such as non-IP networks that cannot support STIR/SHAKEN—or where an illegal call evades such tools.

---

[17] *See Order* ¶ 29.

[18] *Id.* ¶ 36 (noting that such blocking will provide significant consumer protections by "incentivizing upstream voice service providers to better police their networks by raising the cost of passing along bad traffic."). *See id.* ¶¶ 35-45.

[19] *See id.* ¶ 38. For example, in the Department of Justice's complaint against a single gateway provider, it alleged that "the defendants carried 720 million calls during a sample 23-day period." Department of Justice Press Release, *The Department of Justice Files Actions to Stop Telecom Carriers Who Facilitated Hundreds of Millions of Fraudulent Robocalls to American Consumers* (January 28, 2020) ("*DOJ Press Release*"), *available at* https://www.justice.gov/opa/pr/department-justice-files-actions-stop-telecom-carriers-who-facilitated-hundreds-millions).

[20] *See* USTelecom – The Broadband Association, Whitepaper: How to Identify and Mitigate Robocalls, at 7 (Oct. 2019), https://www.ustelecom.org/wp-content/uploads/2019/11/USTelecom-Whitepaper-Combating-Illegal-Robocalls.pdf ("The best place to stop illegal robocall traffic is where it first enters the telephony network through an Originating Provider. Moreover, since this is where the illegal robocall traffic is most concentrated, large volumes of traffic can be stopped before ever reaching consumers.").

B. The Commission's Proposed Safe Harbor for Network-Level Blocking Can Further Enhance Consumer Protections and Incent Voice Service Providers' Robocall Mitigation Strategies.

The same reasons that led the Commission to adopt its existing safe harbors also counsel for the adoption of a safe harbor for network-based blocking of calls that are highly likely to be illegal when such blocking is managed with sufficient human oversight and network monitoring.[21] The Commission is right that "no reasonable consumer would want to receive [such calls]."[22] Illegal calls go far beyond mere annoyances, and can inflict immeasurable damage on their victims, ranging from the loss of financial savings,[23] threats to health,[24] and the diminishment of self-esteem.[25] Given the broad range of detrimental impacts, the Commission can ensure that providers have regulatory certainty to prevent illegal calls from ever reaching consumers. The proposed safe harbor would do just that.

Voice providers have already demonstrated the accuracy, reliability, and value of network-level blocking by identifying billions of illegal calls and preventing them from ever

---

[21] *See FNPRM* ¶¶ 104-06.

[22] *Id.* ¶ 105.

[23] Sarah Krouse, *Robocall Scams Exist Because They Work—One Woman's Story Shows How*, Wall Street Journal (Nov. 21, 2019), *available at* https://www.wsj.com/articles/robocall-scams-exist-because-they-workone-womans-story-shows-how-11574351204) (detailing how a caller impersonating an FBI agent persuaded a woman to lose nearly $340,000 from her bank accounts.).

[24] *See e.g.*, Letter from Rosemary C. Harold, Chief, Enforcement Bureau, FCC and Lois C. Greisman, Associate Director, Division of Marketing Practices, FTC, to Chris Cordero and Scott Ketter, Connexum (April 3, 2020), *available at* https://docs.fcc.gov/public/attachments/DOC-363522A3.pdf) (stating that the robocalls in question included "fraudulent offers of COVID-19 home testing kits," and had "the potential to inflict severe harm on consumers.").

[25] *See e.g.*, Hearing Transcript, Special Committee on Aging, United States Senate, *Still Ringing off the Hook*, at 15 (Oct. 4, 2017) (testimony of Honorable Josh Shapiro, Attorney General, Pennsylvania) stating that "one of the biggest challenges we face on the education front, and from hearing from seniors, is that they are very embarrassed and ashamed when it happens, and I do not think we can underestimate the effect of that."); *see also Elder Fraud*, FBI.gov, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud (last visited August 19, 2020) ("[S]eniors may be less inclined to report fraud because . . . they may be too ashamed at having been scammed. They might also be concerned that their relatives will lose confidence in their abilities to manage their own financial affairs.").

reaching their intended consumer targets. For example:

- AT&T supplements its customer-facing tools with a network-based call blocking program run by its global fraud team that was launched in 2016 on AT&T's wholesale IP platform and subsequently expanded in 2019 to its mobile network. Consistent with the Commission's proposal, "the program relies on curated network intelligence and a highly experienced team of fraud investigators to target suspected illegal high-volume calling events."[26]

- Verizon has instituted a "robust network blocking program" that it emphasizes as having "important consumer protection benefits."[27] Verizon's robust network blocking program has "blocked millions of calls where the calling party number is invalid, unassigned, or where the person to whom the number was assigned has authorized the block."[28] Verizon has also begun "providing blocking in the network of high risk spam calls for customers whose phones do not support the Call Filter app," and it plans to expand the reach of its blocking services going forward.[29]

By combining sophisticated analytics with human oversight and network monitoring, providers' network-level blocking efforts are tailored to narrowly target calls that are highly likely to be illegal, while establishing protections to minimize the risk of erroneous blocking of legitimate calls. Network-level blocking efforts such as these prevent calls from ever reaching consumers, thereby protecting consumers from encountering the risk of fraud or other harms.[30]

While these network-level blocking solutions are already protecting consumers, lingering uncertainty and liability risks limit providers from broader and more robust deployment of this solution. The Commission's proposed safe harbor is needed for voice service providers to

---

[26] Letter from Joan Marsh, Executive Vice President, Regulatory & State External Affairs, AT&T, to Mika Savir, Consumer & Governmental Affairs Bureau, FCC, at 4 (Feb. 28, 2020).

[27] Comments of Verizon, CG Docket No. 17-59, WC Docket No. 17-97, at 3 (filed Jan. 29, 2020) ("*Verizon Comments on Call Blocking Report*").

[28] Letter from Christopher D. Oatway, Associate General Counsel, Federal Regulatory and Legal Affairs, Verizon, to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC, at 3 (Feb. 28, 2020).

[29] *Id.* at 2.

[30] In discussing its cooperation with the Social Security Administration, Verizon noted that it "blocked more than 10 million calls in . . . three months – calls that would otherwise have terminated to U.S. consumers and resulted in substantial financial harm." *Verizon Comments on Call Blocking Report* at 3.

expand robocall mitigation solutions reducing liability concerns associated with network-level blocking, thereby giving providers the necessary flexibility to protect consumers, just as the Commission has done with its prior safe harbor Orders.

The Commission's proposed safe harbor will give providers more confidence to protect consumers by clarifying providers' authority to block calls that are highly-likely illegal at the network-level. The Commission has already confirmed that providers have broad authority to block illegal robocalls because call completion rules do not apply to such calls.[31] Still, there remains uncertainty around calls that are highly-likely illegal in light of the Commission's *2017 Call Blocking Order*, which specifically authorized network-level blocking in particular circumstances.[32] The proposed safe harbor will encourage the broader use of network-level blocking tools by clarifying that voice service providers are shielded from liability when blocking calls they believe are highly likely to be illegal based upon the combination of sophisticated analytics, human oversight, and network monitoring, particularly in instances where providers block calls beyond the categories in the *2017 Call Blocking Order*.[33]

---

[31] *See Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor,* CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd. 4876, ¶ 23, n.53 (rel. June 7, 2019) (explaining that "while voice service providers have a continuing obligation to transmit legal calls, *that obligation does not extend to illegal calls*, calls blocked with consumer choice, or calls for which the Commission has authorized blocking" (emphasis added)) ("*2019 Opt-Out Call Blocking Declaratory Ruling*").

[32] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd. 9706, ¶ 60 (2017) ("*2017 Call Blocking Order*").

[33] Even without a safe harbor, providers have the authority to engage in the blocking of illegal calls. However, a safe harbor would provide clarity for many providers, which could encourage them to take more aggressive action against calls that are highly likely to be illegal. *See, e.g., 2019 Opt-Out Call Blocking Declaratory Ruling* ¶ 2 ("The Commission's 2017 *Call Blocking Report and Order and Further Notice of Proposed Rulemaking* was an important step toward ending the scourge of robocalls, but it did not address instances where fraudsters or other illegal callers spoof legitimate, in-service numbers. Similarly, it left unaddressed cases where fraudsters or other illegal callers do not spoof Caller ID."). Further, in its most recent robocall report, Transaction Network Services estimated that "only 5% of unwanted calls are from invalid/unallocated numbers." *2020 TNS Report* at 18; Comments of AT&T, CG Docket No. 17-59, WC Docket No. 17-97, at 14 (filed July 24, 2019) ("[T]o make a dent in the illegal and unwanted

In the *FNPRM*, the Commission correctly found that no reasonable consumer would want to receive calls that are highly likely to be illegal, and as a result, there is no need for consumers to have the opportunity to opt in or opt out.[34] Indeed, scams and unwanted robocalls continue to be the top complaint to the Commission and one provider estimates that scams and unwanted robocalls cost Americans $10 billion a year.[35] Providers have deliberately designed their network-based blocking solutions that leverage reasonable analytics combined with fraud investigations to focus on protecting consumers from calls that are highly likely to be illegal, put consumers at risk of being defrauded, and no reasonable consumer would want to receive.

Absent a safe harbor, providers face liability risks for taking authorized, reasonable, and targeted actions to prevent illegal calls from reaching consumers, in the event that legal calls are inadvertently blocked. Indeed, many have raised the specter of liability and harm from legitimate voice service provider practices that the Commission and Congress are otherwise promoting.[36] As discussed above, providers and analytics engines go to great lengths to avoid blocking legitimate traffic and have no incentive to engage in over-blocking of calls their subscribers want to receive.[37] Just as the reasonable analytics safe harbor for opt-in and opt-out blocking was needed to ensure regulatory certainty and fill the gap between providers' robust

---

robocalls that are plaguing consumers, voice service providers need to block more calls than just those enumerated in the *2017 Call Blocking Order*.") ("*July 24, 2020 AT&T Comments*").

[34] *FNPRM* ¶ 105.

[35] *See, e.g., Building on the Promise of Call Blocking Blog; T-Mobile Scam Block Announcement.*

[36] *See e.g.*, Letter from Michele A. Shuster, Counsel, Professional Association for Customer Engagement, to Marlene H. Dortch, Secretary, Federal Communications Commission, CG Docket No. 17-59, at 2 – 3 (filed May 29, 2019) (stating that voice providers "are rightly concerned about their potential liability for blocking legitimate calls."); Reply Comments of Twilio Inc., CG Docket No. 17-79, WC Docket No. 17-97, 6-8 (filed Feb. 28, 2020) (explaining that "erroneous blocking and mis-labeling result in real harm with serious consequences" and cataloging alleged instances of such actions).

[37] Voice providers are "consciously targeting only the most egregious and blatantly illegal traffic," and do "not attempt to block 'close calls.'" Comments of AT&T, CG Docket No. 17-59, at 7 (filed Sept. 24, 2018).

authority to block calls and the "real risk of liability" they face for doing so,[38] a network-level safe harbor is needed to further "enable[e] voice service providers to use all available technologies and methodologies at their disposal"—including network-level blocking—"without fear of liability."[39]

The Commission's carefully crafted network-level blocking safe harbor will guard "well-meaning voice service providers from liability when they inadvertently, despite best efforts, block legal calls."[40] Providers have no incentive to block the legitimate calls desired by consumers, and they have worked with their partners and relevant stakeholders across the ecosystem to develop and deploy sophisticated programs to ensure they are targeting and stopping the calls that continue to plague consumers. The Commission's proposed conditions for the safe harbor—which include reasonable analytics, human oversight, and network monitoring—are all meant to identify and narrowly target calls that are highly likely to be illegal and will complement providers' existing efforts and incentives to complete legitimate calls.[41] With this approach, the Commission can strike the right balance of giving providers more tools to protect consumers and limiting the potential for erroneous blocking.

C. The Commission Should Consider Additional Safe Harbors to Further Empower and Protect Consumers as Robocall Mitigation Tools Develop.

While adopting the safe harbors in the *Order* and the network-level blocking safe harbor

[38] *Order* ¶ 23 (stating that "[b]y removing regulatory uncertainty, [the Commission] encourage[s] voice service providers to better protect their customers from unwanted calls.").

[39] *Id.* ¶ 44.

[40] *July 24, 2020 AT&T Comments* at 19. *See also* Ex Parte Presentation of CTIA, US Telecom, and NCTA, at 3 (filed January 31, 2020) (explaining that the authority to block illegitimate calls "is distinct from liability protection for when good-faith actions result in the inadvertent blocking of legitimate calls" and that "[p]roviders need both to unleash all resources against bad actors and to protect consumers.").

[41] *Id.* ¶ 104.

above will help promote providers' efforts to deploy more robust and flexible call-blocking solutions, protecting consumers requires a holistic, multi-pronged approach that can quickly adapt to the ever-changing tactics of illegal robocallers as the Commission acknowledged in the *Order*.[42] Given this tactical reality, the Commission should consider additional safe harbors as robocall mitigation tools develop, beyond to the two safe harbors established in the *Order* and the proposed network-level call-blocking safe harbor.[43] As providers continue to deploy innovative robocall mitigation tools, the Commission should likewise continue to evolve its approach to promoting industry efforts to protect consumers, including by considering new safe harbor mechanisms to effectively address potential regulatory uncertainties and liability concerns. The absence of such safe harbors could effectively chill the broad adoption and deployment of other tools, beyond existing call blocking tools.

The Commission should therefore continue to develop its record on additional safe harbors and take appropriate action as necessary. For example, to ensure that trust identification tools like STIR/SHAKEN attestation can continue to empower and protect consumers as industry's authentication solutions develop and evolve, the Commission should consider a safe harbor "for the unintended or inadvertent misidentification of the level of trust for individual calls," as contemplated under the TRACED Act.[44] By continuing to implement the TRACED Act and encouraging industry innovation and robocall mitigation efforts, the Commission can help ensure that government and industry collectively can remain ahead of the bad actors and

[42] *Order* ¶ 2.

[43] *See FNPRM* ¶ 87.

[44] TRACED Act § 4(c)(1)(B) (directing the Commission no later than one year after enactment of the TRACED Act to, "establish[] a safe harbor for a provider of voice service from liability for unintended or inadvertent blocking of calls or for the unintended or inadvertent misidentification of the level of trust for individual calls based, in whole or in part, on information provided by the call authentication frameworks.").

continue protecting consumers.

III. AS VOICE SERVICE PROVIDERS WORK TO COMPLETE LEGITIMATE CALLS, THE COMMISSION SHOULD CONTINUE TO PROMOTE FLEXIBILITY IN ROBOCALL MITIGATION AND BLOCKING REDRESS PROGRAMS.

Throughout its efforts to combat abusive robocalls, the Commission has consistently applied a principle of regulatory flexibility that encourages voice service providers to deploy innovative robocall mitigation solutions and redress options and balance protections for consumers and legitimate callers. Regulatory flexibility has enabled voice service providers to nimbly respond to consumer demand and preferences regarding the calls they want labeled or blocked, while also protecting consumers from the evolving tactics used by fraudsters and abusive robocallers.[45]

For example, in the *Order,* the Commission acknowledged that giving "voice service providers flexibility in how to incorporate authentication into [providers'] analytics" and "flexibility to adapt [providers'] blocking to evolving call patterns" would be key to ensuring that robocall mitigation tools can reflect and respond to the changing robocall landscape.[46] The Commission has also taken a balanced approach to avoid rigid regulation of redress mechanisms that address claims of erroneous blocking by legitimate callers. For instance, in its *Order*, the Commission opted to foster industry use of a range of tools and approaches that make the most

[45] Encouraged by Commission efforts and unconstrained by unnecessarily prescriptive limitations to date, "voice service providers and third-party analytics companies are offering their customers a variety of options for call blocking and labeling" and are "blocking and labeling billions of unwanted calls to American consumers each year." *Report on Call Blocking* ¶ 20; ¶ 57.

[46] *Order* ¶¶ 29, 50. *See also 2019 Opt-Out Call Blocking Declaratory Ruling* ¶ 34 ("We recognize that limiting opt-out call-blocking programs to rigid blocking rules that prescribe in detail when a voice service provider may block is unnecessary when consumers have the option to opt out, 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.").

sense to protect both consumers and legitimate callers.[47]

The Commission should maintain regulatory flexibility as it encourages the deployment of robocall mitigation tools, including labeling, and seeks to ensure adequate redress mechanisms for legitimate callers. By promoting technological innovation and diverse approaches to fight robocalls, the Commission can best equip providers to protect consumers, fight the bad actors behind illegal and unwanted robocalls, and address potential issues regarding reported erroneous blocking of legitimate calls.

A. Any Commission Action Related to Providers' Unique Robocall Mitigation Programs Should Promote Adaptability and Innovation.

The Commission seeks comment on regulating several aspects of providers' anti-robocall efforts beyond call-blocking, including steps providers should take to mitigate bad traffic and to prevent illegal calls from new customers.[48] As CTIA has highlighted throughout this proceeding, wireless voice service providers and their partners throughout the industry have been focused on protecting consumers from abusive robocalls with multi-pronged and varied programs, and the Commission should continue to promote a diverse range of approaches rather than adopt prescriptive requirements.

Among many efforts, wireless voice service providers are long-standing, active members of the Commission's designated traceback consortium, have established robocall mitigation programs, and implemented know-your-customer best practices. Industry has also been working with other stakeholders and the Commission as issues arise, such as supporting the Commission's efforts to crack down on COVID-related fraud perpetrated via robocalls or one-

[47] *Order* ¶ 59 ("We agree with commenters that support allowing voice service providers flexibility for now and pending further developments in the record.").

[48] *See FNPRM* ¶¶ 95-103.

ring scams, participating in traceback efforts, or addressing gateway provider concerns. This voluntary, holistic approach by each provider, paired with collective industry action and collaboration with the Commission, has enabled providers and their partners to protect consumers from tens of billions of illegal and unwanted robocalls.[49]

As these approaches are working to reduce unwanted and illegal robocalls, the Commission should continue to encourage providers to develop their own approaches to mitigating illegal and unwanted robocalls and protecting consumers, rather than adopt restrictive requirements to promote or regulate particular practices.[50] Instead, the Commission should take additional steps to protect consumers by also promoting flexibility in the implementation of STIR/SHAKEN;[51] encouraging voice service providers to block illegal, one-ring scam calls pursuant to their broad authority;[52] and encouraging voluntary and nimble deployment of robocall mitigation tools and programs.[53] Consistent with the TRACED Act, the Commission

[49] *See* Comments of CTIA, CG Docket No. 20-93, at (filed June 19, 2020) ("*CTIA One-Ring Scams Comments*").

[50] The Commission has repeatedly opted against approaches that may "reduce the flexibility of call-blocking programs" and should stay the course. *See, 2019 Opt-Out Call Blocking Declaratory Ruling* ¶¶ 28. *See also id.* ¶ 34 (34 (discussing the importance of flexibility to providers' robocall blocking programs); *2017 Call Blocking Order* (making clear that the call blocking rules adopted therein were "permissive" and "voluntary").

[51] *See* Comments of CTIA, WC Docket Nos. 17-97, 20-67, at 2 (filed May 15, 2020) ("*CTIA STIR/SHAKEN Comments*") (supporting "the Commission's proposal to mandate implementation of the STIR/SHAKEN framework, as Congress directed in the TRACED Act, with appropriate flexibility to encourage innovation and to allow providers to address the various challenges of applying this approach to legacy voice calling services"); Reply Comments of CTIA, WC Docket Nos. 17-97, 20-67, at 3 n.4 (filed May 29, 2019) ("*CTIA STIR/SHAKEN Reply Comments*") (explaining flexibility is key as the "voice services ecosystem continues to work through challenges and develop best practices for call authentication" and showing strong record support for flexibility).

[52] *See CTIA One-Ring Scams Comments* at 3, 5 ("[U]rg[ing] the Commission to continue supporting providers' call-blocking efforts and the development of other best practices to protect consumers from one-ring scams and other illegal and unwanted robocalls.").

[53] *See CTIA STIR/SHAKEN Comments* at 3 ("Given the diverse ecosystem of robocall migitation tools and practices industry is developing to protect consumers, the Commission should refrain from prescribing specific robocall mitigation programs and should allow such providers to draw from the growing diversity and sophistication of anti-robocall tools and approaches available.").

should continue empowering providers to further protect consumers, in lieu of requiring particular practices.

B. The Commission Should Encourage Innovative Labeling Tools that Empower Consumers and Promote Flexible Redress Options for Legitimate Calling Parties to Work with Voice Providers to Resolve Reports of Erroneous Call Blocking.

Wireless voice service providers and their analytics partners want to protect legitimate calls. Wireless providers work with each other and call originators to limit the impact of possible erroneous blocking and mislabeling and addressing issues as they arise. For example, providers and analytics engines work proactively to provide calling parties with best practices to avoid having their legitimate calling campaigns look like unwanted or illegal calls.[54] Additionally, wireless service providers and ecosystem stakeholders are working to develop call authentication best practices, technical solutions, and enhanced standards that will further improve caller identification information and call labeling solutions for consumers.[55] If issues do arise, providers and their analytics partners have designated points of contact for redress mechanisms.[56] Accordingly, no additional Commission action is necessary to address either erroneous mislabeling or blocking of legitimate calls.

---

[54] *See, e.g.*, Best Practices, Verizon, https://www.voicespamfeedback.com/vsf/bestPractices; Comments of Transaction Network Services, Inc., CG Docket No. 17-59, WC Docket No. 17-97, at 14–15 (filed Jan. 29, 2020); Reply Comments of AT&T., WC Docket Nos. 17-97, 20-67, at 21 (filed May 29, 2020) (discussing "AT&T's ongoing and constructive dialogue with call originators and its ongoing work with its analytics partner") ("*AT&T STIR/SHAKEN Reply Comments*"); Comments of T-Mobile, CG Docket No. 17-59, at 2 (filed Sept. 24, 2018) ("T-Mobile is continuously working to further refine its modeling and analysis and to quickly correct any circumstance where calls have been incorrectly categorized as potentially fraudulent. T-Mobile's vendor, First Orion, offers a platform (www.calltransparency.com) that enables call originators to proactively engage to minimize any issues."); *see also* Comments of T-Mobile, CG Docket No. 17-59, WC Docket No. 17-97, at 8 & n.22 (filed Jan. 29, 2020).

[55] Registries are emerging as a leading solution to enhance call authentication and strengthen labeling and display solutions. *See* IP-NNI Task Force Mission, ATIS, https://www.atis.org/01_strat_init/ip-nni/mission/ (last visited May 21, 2020) (noting that IP-NNI task force is working on "[a]chiev[ing] consensus on a registry approach to support routing of E.164 number-address named SIP sessions.").

[56] *Report on Call Blocking* ¶ 66.

The Commission seeks comment on whether action is needed to address mislabeling of calls.[57] As CTIA has previously explained, the Commission should remain focused on promoting innovation and experimentation in call labeling to empower and protect consumers, rather than imposing any requirements at this time.[58] Call labeling, which is deployed by "[m]ost voice service providers and analytics companies"[59] including CTIA's member companies, offers a variety of options to inform and empower consumers, and has proven popular. Labeling uses various technologies, including "artificial intelligence, machine learning, and call behavior as part of the reasonable analytics."[60] Moreover, labeling solutions can be deployed across legacy networks, benefiting customers on IP and non-IP networks alike. Providers have lauded "flexibility in call labeling as part of providers' ability to differentiate their services,"[61] and are "taking advantage of the flexible regulatory environment that the Commission has fostered . . . to refine and expand" call labeling.[62] In the event that issues regarding mislabeling may arise, providers and analytics engines have dedicated resources and mechanisms to quickly respond to reported issues.[63] Given that innovation and market incentives are helping providers deliver various tools to consumers, and providers have redress

[57] *See FNPRM* ¶ 109 ("We seek comment on whether we should address the issue of mislabeling of calls and, if so, how.").

[58] *See CTIA STIR/SHAKEN Comments* at 12-14.

[59] *Id.* at ¶ 10. *See also id.* Appendix B (charting labeling approaches across the ecosystem)

[60] *Report on Call Blocking* ¶ 35.

[61] Reply Comments of T-Mobile USA Inc., WC Docket Nos. 17-97, 20-67, at 7 (filed May 29, 2020).

[62] *AT&T STIR/SHAKEN Reply Comments* at 21.

[63] *See CTIA STIR/SHAKEN Reply Comments* at 7 (explaining that "wireless providers and their analytics partners are working to address reports of mislabeling, inadvertent blocking, or other issues"). Some programs enable calling parties to register to avoid inadvertent mislabeling. *See e.g.,* Communications Sector Coordinating Council, Using Autodialers for COVID-19 Related Public Service Announcements, https://www.iaem.org/Portals/25/documents/Using_Autodialers_for_COVID-19_PSAs.pdf (listing portals for "registering legitimate numbers").

options in place, the Commission should maintain its current approach.

With respect to erroneous blocking of legitimate calls, the Commission was right to promote flexibility in the *Order* as redress solutions and best practices develop, and it should maintain that approach going forward.[64] Indeed, the Commission already addressed redress as contemplated in Section 10 of the TRACED Act in the *Order*, and need not impose "more extensive" and prescriptive requirements on voice service providers,[65] because doing so would constrain solutions and may stifle innovation.

For example, the Commission proposes to require voice service providers "to provide a list of individually blocked calls that were placed to a particular number at the request of a subscriber to that number."[66] The Commission should not adopt this requirement. In addition to other mechanisms, a blocked call list may help enable bad actors to learn which numbers are being blocked, enhancing their ability to pivot to different phone numbers and evade robocall mitigation tools—a concern the Commission has already recognized.[67] Additionally, the record does not demonstrate that consumers demand information about missed robocalls. To the contrary, consumers' primary complaint continues to be too many illegal and unwanted calls, while the claims of blocking in error—which fuel requests for redress mandates—come from calling parties.[68]

---

[64] *Order* ¶ 59

[65] *Id.* ¶ 4; *FNPRM* ¶ 90.

[66] *FNPRM* ¶ 111.

[67] *See Order* ¶ 59 (similarly recognizing that providing information to bad actors is "potentially harmful").

[68] As the FCC has observed, reports of false positive blocking "may result from consumers choosing not to answer calls from numbers they do not recognize and allowing the call to go to voicemail instead." *Report on Call Blocking* ¶ 60.

IV. CONCLUSION.

CTIA appreciates the Commission's leadership in the continued fight to protect consumers from unwanted and illegal robocalls, and the wireless industry shares the Commission's commitment and focus. The safe harbors for call blocking that the Commission adopted in recent Orders are an important step forward in this ongoing effort that enable and incent voice service providers to take aggressive and innovative actions to protect consumers. CTIA urges the Commission to build on this progress by adopting a network-level blocking safe harbor to enhance consumer protections and maintain providers' flexibility in deploying robocall mitigation solutions and protecting legitimate calls through call-blocking redress solutions. With additional regulatory incentives and the flexibility necessary to deploy and evolve innovative solutions, CTIA's member companies can continue to take additional actions to empower and protect consumers from unwanted and illegal robocalls.

Respectfully submitted,

/s/ Sarah Leggin

Sarah K. 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

August 31, 2020