Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls Consumer and Governmental Affairs Bureau Seeks Input to Refresh the Record on Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59 DA 18-842

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Krista L. Witanowski
Assistant Vice President, Regulatory Affairs

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

September 24, 2018

TABLE OF CONTENTS

Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls Consumer and Governmental Affairs Bureau Seeks Input to Refresh the Record on Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59 DA 18-842

COMMENTS OF CTIA

I. INTRODUCTION AND SUMMARY.

CTIA[1] appreciates continued focus from the Federal Communication Commission ("FCC" or "Commission") on illegal robocall abatement and welcomes the opportunity to respond to the Consumer and Governmental Affairs Bureau's August 10, 2018 *Public Notice* to refresh the record regarding "empower[ing] voice service providers to block illegal calls."[2] Industry and the FCC share a common objective: stopping illegal calls. As conveyed to the Commission through multiple filings in this and related dockets by CTIA and its individual members, the wireless industry continues to aggressively mitigate illegal robocalls. These efforts

[1] 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] *Consumer and Governmental Affairs Bureau Seeks to Refresh the Record on Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Public Notice, DA 18-842, at 1 (Aug. 10, 2018) ("*Public Notice*").

are still in their early stages and the results of industry and FCC action have yet to be fully realized. As the Commission considers the record, three main principles should inform its work:

- The Commission must give industry the ***regulatory flexibility*** to respond to consumer demands and address illegal robocalling challenges in creative and dynamic ways. This will allow industry to stay ahead of the bad actors who quickly adapt technologies and techniques that continue to plague U.S. consumers with illegal calls. This means that the Commission must remove barriers to industry innovation; it is critical that the FCC avoid heavy-handed regulation and onerous reporting requirements. CTIA is encouraged that the *Public Notice* states the Commission's intention is to "ensure[] providers have sufficient flexibility available to adapt to dynamic calling patterns."[3]
- Providing ***robust safe harbors*** for industry actors to aggressively combat illegal robocalls is the most effective way to encourage the behavior that the Commission wants to see from carriers, protect responsible carriers from liability, and continue to give industry the flexibility it needs to innovate.
- Carrier-initiated blocking can be a useful tool, but it is not a panacea. To effectively protect U.S. consumers from illegal robocalls, the FCC must embrace the ***multi-pronged approach*** being adopted by industry. No individual carrier's approach against illegal robocallers needs to look the same as any other. Across the many players in the ecosystem (*e.g.*, small and large carriers, call blocking application providers, and third-party data analytics providers), there is innovation and action at every stage in call transmission. And, because illegal robocallers change their tactics as industry continues to improve, flexibility and adaptability are key. The FCC should not put undue weight on any single tactic, actor, or stage—a holistic approach is a better answer to the scourge of illegal robocalling.

With these principles in mind, CTIA urges the Commission to (1) authorize broader call-blocking and (2) protect carriers with robust safe harbors. In addition, the FCC should encourage multiple techniques and technologies to combat illegal robocalling including: know-your-customer practices, stipulations in contracts, SHAKEN/STIR, tools that enable consumers to label and block illegal robocalls, consumer education, and traceback. Finally, the Commission should not take a regulatory approach based on the perceived problem of erroneous labeling and blocking, which needs to be better contextualized and understood.

[3] *Id.* at 1.

II. CARRIER-INITIATED BLOCKING IS A KEY PART OF THE OFFENSIVE AGAINST ILLEGAL ROBOCALLS, BUT IT IS NOT A PANACEA.

Industry is engaged in carrier-initiated blocking[4] pursuant to the *2017 Call Blocking Order*,[5] which authorized voluntary carrier-initiated blocking in a limited number of circumstances.[6] Major carriers have embraced those activities. 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."[7] 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."[8] T-Mobile reports that it has blocked 986 million calls in the year ending August 31, 2018.

Carrier-initiated blocking is not a panacea. While carrier-initiated call blocking can be part of a strategy against illegal robocalls, there may be reasons not to devote resources to this type of blocking at the network level. For example, bad actors develop strategies to work around blocking, leading to different illegal robocall challenges. Since spring of 2017, when some

---

[4] The *Public Notice* is primarily focused on carrier-initiated blocking. *See id.* at 1, n.1 ("While third-party apps and other tools can help consumers avoid illegal calls, our focus here is voice service provider blocking of illegal calls without consumer consent or opt-in."). CTIA discusses third-party blocking and labeling services and customer opt-in services in Section IV.B.

[5] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and FNPRM, 32 FCC Rcd. 9706 (Nov. 17, 2017) ("*2017 Call Blocking Order*").

[6] *Id.* ¶¶ 18-40 (establishing permissive, carrier-initiated blocking of (1) calls purporting to originate from invalid numbers, (2) calls purporting to originate from numbers not allocated to any provider, and (3) calls purporting to originate from numbers that are allocated but unused). The *2017 Call Blocking Order* additionally authorized blocking at the request of the subscriber holding the originating number. *Id.* ¶¶ 10-17.

[7] Comments of AT&T, CG Docket No. 17-59, at 9 (July 20, 2018) ("*July 20, 2018 AT&T Comments*").

[8] *Id.* at 10.

carriers increased call blocking, there has been a rise in neighbor spoofing, which is a tactic used by robocallers to "display[] a phone number similar to [the consumer's] on [the consumer's] caller ID, to increase the likelihood that [the consumer] will answer the call."[9]

For these reasons, some carriers that are aggressively combatting illegal robocalls have opted not to engage in the blocking permitted by the *2017 Call Blocking Order*. For example, Sprint has explained that

> "[it] has not implemented blocking of invalid, unallocated, or unassigned numbers despite the Commission's order permitting it to do so. Sprint's data does not show that robocalls from these numbers constitute a significant part of the problem. Blocking them would also increase spoofing as illegal call originators would shift their efforts to spoofing legitimate numbers. This spoofing causes harm to the owner of the spoofed number because its outgoing calls may be blocked or improperly identified as robocalls, and the owner may receive complaints from call recipients who falsely assume that the owner of the originating number was responsible for placing the illegal and unwanted calls."[10]

III. THE COMMISSION SHOULD AUTHORIZE ADDITIONAL BLOCKING AND PROVIDE SAFE HARBORS TO CARRIERS THAT CHOOSE TO ENGAGE IN CALL BLOCKING.

A. The Commission Should Authorize Voluntary Blocking Based on a Carrier's Good Faith Determination That a Call Is Illegal, Coupled With a Robust Safe Harbor.

The *2017 Call Blocking Order* was a step in the right direction, but the Commission should do more to empower carriers to combat illegal robocalling. The FCC should broadly authorize voluntary carrier-initiated blocking and not limit its authorization to calls originating from narrow categories of numbers. Specifically, the Commission should give its blessing to *any* carrier-initiated blocking that results from procedures that are reasonably likely to confirm that blocked calls are illegal robocalls, so long as the carrier has a good-faith reason to believe that

[9] *See Spoofing and Caller ID*, FCC Consumer Guide, https://www.fcc.gov/consumers/guides/spoofing-and-caller-id (last updated July 25, 2018).
[10] Comments of Sprint, CG Docket No. 17-59, at 5 (July 20, 2018).

the call was an illegal robocall, the carrier followed its procedures, and the carrier has a process in place to unblock legal callers that might be inadvertently blocked.[11]

In authorizing a permissive call blocking scheme, CTIA urges the Commission *not* to dictate specific criteria but, instead, to allow carriers to make call blocking determinations.[12] Blocking decisions vary based on a number of factors, not least of which is the unique network over which calls are transmitted. Industry—not the Commission—is in the best position to develop standards that indicate a call is likely to be illegal. Carriers can identify emerging calling patterns and develop tools to address them using network statistics, customer feedback, and other methods tailored to each network. For example, AT&T has explained that "multiple conditions on [its] network may trigger a number for investigation," including low average call duration; call completion ratios; invalid numbers placing large volumes of calls; common Caller ID Name (CNAM) values across service providers; large bursts of calls in a small time window; large volumes of complaints related to a suspect robocaller line; sequential dialing patterns; neighbor spoofing patterns; patterns that indicate TCPA and other contract violations; correlation of AT&T network data with complaint data from regulators, customers, and other carriers; and numbers dialed with lines on the FTC Do Not Call list.[13] Similarly, T-Mobile offers a network-based solution that relies on a wide variety of data and sophisticated analytics to determine that a call is likely fraudulent.[14] Notably, some of these factors that are indicia of illegal robocalling

[11] *See July 20, 2018 AT&T Comments* at 14.
[12] The *Public Notice* asks about specific criteria that may be used by carriers to block illegal robocalls from reaching consumers. *Public Notice* at 2.
[13] *See* AT&T Ex Parte, CG Docket No. 17-59, at 4 (Mar. 6, 2018) ("*March 6, 2018 AT&T Ex Parte*").
[14] *See* 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).

may also be associated with legal robocalling, underscoring the need for flexibility, adaptation, and discretion in carrier blocking practices.

The Commission should couple a permissive call-blocking authorization with a robust safe harbor to promote carrier-initiated call blocking. Blocking is generally at odds with the concept of common carriage and the "strong policy against allowing voice service providers to block calls."[15] A robust safe harbor will help overcome this barrier.[16] CTIA reiterates the need for a safe harbor for carrier-initiated call blocking, as detailed in earlier comments.[17] The FCC should adopt a safe harbor providing that:

- ***Where a carrier engages in good-faith call blocking, the carrier is not liable for any call that is not completed as a result.*** As call blocking has increased, so too has the real and significant liability risk associated with it. Carriers have seen increased litigation threats and activity in connection with efforts to mitigate illegal robocalls. The Commission should adopt a rule 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 and reasonable belief that such blocking is permissible under FCC rules. This rule would protect carriers from liability and encourage more aggressive carrier action to thwart illegal activity.

- ***Sharing of CPNI among carriers for the purpose of call blocking is permissible under Section 222 of the Communications Act.*** The Commission should make clear that Section 222(d) is not an impediment to information sharing, including of CPNI, to address cyber and network security threats, as well as to detect and prevent fraud against consumers. The *2017 Call Blocking Order* took a step in the right direction by confirming that "voice service providers are free to share DNO ["Do-Not-Originate"] requests as necessary to block calls in the limited circumstances identified in this Report and Order"[18] and noting that "information sharing required for traceback or other

[15] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Notice of Proposed Rulemaking and Notice of Inquiry, 32 FCC Rcd. 2306, ¶ 9 (Mar. 23, 2017).
[16] Additional protections beyond excluding blocked calls from applicable call-completion requirements are necessary. *See 2017 Call Blocking Order* ¶ 30 ("The Report and Order clarifies the call completion rules by allowing, but not requiring, voice service providers to exclude calls blocked under these new rules from their call completion calculations, to the extent that they are aware of which calls are blocked.").
[17] Comments of CTIA, CG Docket No. 17-59, at 13-16 (June 30, 2017).
[18] *2017 Call Blocking Order* ¶ 53.

robocall abatement" is permitted under Section 222;[19] however, carriers need broader, more explicit, and more robust CPNI protections. CTIA urges the Commission to take the approach here that it did in the *2016 Privacy Order*, permitting carriers to share CPNI to "protect the rights or property of the telecommunications carrier, or to protect users of the telecommunications service and other providers from fraudulent, abusive, or unlawful use of the service,"[20] including "fraudulent, abusive, or otherwise unlawful robocalls."[21] Without clear protection, carriers may hesitate to share information, hindering robocall abatement efforts.

- ***Where there are multiple users on an account – such as a family plan or enterprise account – a carrier may block when directed by the authorized account holder.*** The *2017 Call Blocking Order* authorizes voluntary carrier-blocking of numbers where the subscriber to those numbers submit DNO requests. One criterion for this type of voluntary blocking is that the "subscriber to the number must authorize it to be blocked."[22] CTIA urges the Commission to adopt clear "rules of the road" regarding subscriber authorization to avoid disputes and other administrative challenges regarding customer authorization. Drawing a clear line allowing authorized account holders to make DNO requests is especially important in multi-line contexts, *e.g.*, family, business, or enterprise plans.

When industry asked the FCC to establish a robust safe harbor in connection with the blocking authorized in 2017, the Commission declined to do so "because [it did] not have a sufficiently developed record on the subject."[23] The record, now refreshed, provides ample basis for the Commission to act to provide robust protections for good-faith actors in this ecosystem. By providing robust protections, industry will be more likely to expand blocking to combat bad actors in an effort to protect consumers.

[19] *Id.* ¶ 53, n. 143.
[20] 47 C.F.R. § 64.2004(a)(3) (overturned by Congressional Disapproval of a Rule Submitted by the Federal Communications Commission, Pub. L. No. 115–22 (2017)).
[21] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, 31 FCC Rcd. 13911, ¶ 213 (Nov. 2, 2016) ("*Broadband Privacy Order*"). The Commission noted in the *2017 Call Blocking Order* that the *Broadband Privacy Order* "was disapproved by Congress pursuant to the Congressional Review Act, so the interpretation espoused there has no effect." *2017 Call Blocking Order* ¶ 52, n.140.
[22] *2017 Call Blocking Order* ¶ 13.
[23] *Id.* ¶ 9, n.28.

B. The FCC Should Not Move Toward a Regulatory Model of "Enforceable" Criteria for Blocking.

Rather than asking about safe harbors, the *Public Notice* suggests that the Commission should adopt "specific, enforceable criteria . . . to prevent improper blocking."[24] CTIA urges the Commission not to move toward a more regulatory approach by mandating specific criteria.

First, the *Public Notice* correctly notes that "enshrining blocking criteria in the Commission's rules would enable illegal callers to circumvent them."[25] Bad actors will innovate around rule-based criteria and this would have the unintended consequence of making the challenge worse by limiting industry flexibility to adapt. The Commission should not give bad actors a roadmap to victimize consumers. Second, Commission standardization of call blocking criteria would be ineffective and unwise. As discussed above, there is no one-size-fits-all solution for carriers, which makes this an area unsuitable for prescriptive regulation in the form of "specific, enforceable criteria." Finally, the FCC should not add regulatory demands to call blocking, which would create another barrier to carrier-initiated call blocking and undermine the Commission's attempts to encourage carrier-initiated blocking in spite of the general federal policy against blocking.

IV. OTHER SOLUTIONS ARE PROMISING BUT WILL REQUIRE REGULATORY FLEXIBILITY AND SAFE HARBORS.

The *Public Notice* asks: "Are there other actions, including traceback, that providers could take that would stop [illegal] calls from reaching consumers in the future?"[26] The answer is a resounding yes. Industry is taking a multi-pronged approach to illegal robocalling, from call origination to termination, to address multiple stages of illegal call transmission. No solution—

[24] *Public Notice* at 2.
[25] *Id.*
[26] *Id.* at 2-3.

blocking or otherwise—is a silver bullet. Techniques evolve and it is still too early to tell which tools will have the biggest impact.[27] The Commission should support efforts to fight illegal robocalling at every point of transmission.

A. Service Providers Are Using Aggressive Practices To Stop Illegal Robocalls at the Source, Before They Are Originated.

In addition to empowering providers to block traffic prior to termination (receipt), the Commission should support steps to ensure that service providers do not originate illegal traffic in the first place. The Commission should support industry efforts to prevent this practice.

1. Industry is developing "Know-Your-Customer" best practices.

Know-Your-Customer protocols allow voice providers to take steps to avoid providing high-volume calling services to illegal robocallers at the origination stage, rather than waiting until calls are transmitted and having to block them at the terminating (receiving) stage. Illegal robocall schemes typically have certain characteristics: high volume, short duration, and limited successful attempts. They also may be characterized by inconsistent originating caller-ID information. Carriers can analyze call origination based on these characteristics and investigate suspicious patterns. Carriers have terms of service that prohibit their customers from using their networks for illegal activities and can police bad actors (based on calling patterns) accordingly.

Verizon has developed Know-Your-Customer procedures based on readily-calculated traffic metrics. Verizon begins by running daily analytics on all customers served on Internet Protocol platforms (wholesale and retail customers) to look for patterns that are consistent with illegal robocalling activity. Verizon develops a Robo Score[28] for all customers, and then takes a

[27] The *Public Notice* goes on to ask: "Are some actions more likely to be effective than others?" *Id.* at 3.

[28] Verizon calculates the Robo Score using standard data elements that all voice providers have in their systems:

closer look at customers that originate calls beyond certain thresholds. Specifically, for customers with high Robo Scores, Verizon performs additional analytics regarding (1) volume, (2) velocity, (3) neighbor-ness score, and (4) spam score. After these analytics, if a customer is a concern, Verizon engages with them directly and requires them to justify the legality of their traffic.[29]

As with carrier-initiated call blocking, the Know-Your-Customer approach will benefit from regulatory flexibility instead of any type of mandate. First, there is not yet industry consensus on Know-Your-Customer best practices. Know-Your-Customer practices may be unnecessary for some carriers. One obvious example is a service provider that does not originate *any* robocall traffic—legal or illegal—which makes it unnecessary to implement Know-Your-Customer practices. Other carriers may have alternative, equally valid and effective methods to achieve the same outcome as Know-Your-Customer practices, that is, to prevent origination of illegal calls. Second, Know-Your-Customer solutions are evolving. Third parties are working to independently vet call originators. These entities may further develop Know-Your-Customer best practices. Regulatory flexibility is needed to allow Know-Your-Customer best practices to reach their full potential.

> "each customer's unanswered rate (including calls that calling parties choose not to answer, calls the caller cancels, and calls to unassigned numbers) and its average call duration. The unanswered rate is an indicator of how willing call recipients are to pick up their phone for a caller, as well as the extent to which a caller may be "carpet-bombing" large swaths of numbers that are not even assigned to anyone. The average call duration is an indicator of how long call recipients stay on the line when they do answer the call. [Verizon] combine[s] the unanswered rate and call duration into a single score, with higher scores representing behavior that is more consistent with (but is not necessarily indicative of) patterns known to be associated with illegal robocalling."

See July 20, 2018 Verizon Comments at 12.

[29] *See id.*

To the extent that there is a role for the FCC, it may consider encouraging more carriers to implement reasonable practices to scrutinize call originators. The Commission should not impose prescriptive rules, but it should make clear to carriers offering high-volume call origination services that Know-Your-Customer (or similar) procedures are favored.

There are other ways that the Commission can address these issues. For example, T-Mobile argued in another proceeding for the Commission to adopt a "Safe Harbor Point of Interconnection (POI) Solution" for interconnection to help with the transition to IP services and reduce intercarrier compensation disputes. T-Mobile argued that the status quo, requiring carriers to establish one point of interconnection in each local access and transport area, enabled traffic pumping and robocalling. T-Mobile asserted that its proposed solution would help to "fight robocalling, spoofing, fraud and other harmful practices," because the vast majority of illegal robocalls do not come from direct interconnection.[30]

2. **Carriers are fighting illegal robocalling via contracts.**

Additionally, in the context of high-volume calling services, some carriers have begun to stipulate—either through terms of service and/or contract amendments—that upstream providers, by sending calls to the carriers, agree to (1) undertake a minimum level of Know-Your-Customer and follow-the-rules diligence; (2) cooperate with industry traceback efforts, and (3) impose these same requirements on any providers for whom they serve as an intermediate carrier in sending calls onward to a consumer. Carriers are also looking at tariff approaches to achieve similar outcomes.[31] Such efforts are to be commended and encouraged.

---

[30] Comments of T-Mobile, WC Docket No. 18-155, at 20 (July 20, 2018).

[31] Comments of Verizon, CG Docket No. 02-278, at 3-4, n.6 (Jan. 23, 2015) ("Similarly, when a suspicious traffic pattern arrives on Verizon's network via one of Verizon's wholesale customers, Verizon contacts the wholesale customer to request that the wholesale customer immediately investigate such traffic and ascertain whether the traffic is legitimate and, if not, to cease transmitting such traffic to Verizon. . . . To the extent Verizon were to learn of suspicious

B. Innovation Is Empowering Consumers To Mitigate Illegal Robocalling.

Despite strides in mitigating illegal robocalling before calls reach the network, illegal traffic will inevitably be originated. So, carriers and others are developing tools that empower consumers to identify and thereby prevent unwanted, illegal calls: SHAKEN/STIR, call labeling, and consumer-initiated and opt-in blocking. Industry is also prioritizing consumer education about these and other tools.

1. Industry-driven SHAKEN/STIR is a next-generation anti-robocall measure that will be implemented as early as next year.

SHAKEN/STIR is a set of leading-edge cryptographic protocols and operational procedures to authenticate calls and mitigate spoofing and associated illegal robocalling. SHAKEN—which stands for "**S**ignature-based **H**andling of **A**sserted information using to**KEN**s"—and STIR—which stands for "**S**ecure **T**elephone **I**dentity **R**evisited"—were industry-developed through a consensus process led by ATIS and the SIP Forum. As explained in the Robocall Strike Force Report, these protocols will enable "verif[ication] and authenticat[ion] [of] caller identification for calls carried over an Internet Protocol (IP) network."[32] The report notes that, "the deployment of these standards under a sound governance framework will result in higher end user confidence in the identification of incoming IP-only voice calls."[33]

There has been significant progress on the call authentication trust anchor (CATA), whose primary goal is "to ensure the integrity of the issuance, management, security and use of [the] STI certificates" that are at the heart of the SHAKEN/STIR technologies.[34] On December

---

traffic patterns generated by a Verizon retail customer, we would similarly pursue appropriate remedies as permitted by law and by applicable contracts and tariffs.").

[32] *Robocall Strike Force Report*, FCC, at 3 (Oct. 26, 2016) ("*2016 Robocall Strike Force Report*"), https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf.

[33] *Id.*

[34] *Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR*, NANC Call Authentication Trust Anchor Working Group, at 4 (May 3, 2018) ("*CATA Working*

7, 2017, less than 90 days after the close of the comment cycle for the Notice of Inquiry in Docket No. 17-97, the Wireline Competition Bureau requested that NANC establish a CATA Working Group to address the policy and logistical processes for standing-up the Governance Authority specified by the SHAKEN/STIR standard. On May 3, 2018, NANC's CATA Working Group submitted its *Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR* ("*CATA Working Group Report*"), including recommendations for an industry-led entity to govern the SHAKEN/STIR ecosystem.[35] Chairman Pai promptly accepted these recommendations.[36]

In the short time since the *CATA Working Group Report* was issued, significant progress is underway. Pursuant to Section 3 of that report, industry stakeholders from trade associations representing a variety of industry segments and Founding Members agreed that the Governance Authority ("GA") should be set up under the auspices of ATIS. ATIS accepted that stakeholder consensus. There have been over 14 meetings held over 11 weeks and on August 29, 2018, ATIS announced that the GA Board has been stood-up and that it had finalized its budget and budget allocation methodology, Board make-up, corporate structure, and Operating Procedures.[37] The GA Board also established a Technical Committee, as well as its RFP Task

---

Group Report"), http://www.nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf .

[35] *Id.*

[36] Press Release, FCC, *Chairman Pai Welcomes Call Authentication Recommendations from the North American Numbering Council* (May 14, 2018), https://www.fcc.gov/document/chairman-pai-welcomes-call-authentication-framework.

[37] ATIS Ex Parte, CG Docket No. 17-59 (Sept. 13, 2018) ("Immediately following the delivery of the NANC CATA WG report to the CFC in May, industry stakeholders mete several times per week to collectively establish and launch the STI-GA."); Press Release, ATIS, *Secure Telephone Identity Governance Authority Launched In Major Industry Effort to Combat Unwanted Robocalling* (Sept. 18, 2018), https://sites.atis.org/insights/secure-telephone-identity-governance-authority-launched-in-major-industry-effort-to-combat-unwanted-robocalling/.

Force to prepare to issue an RFP for a Policy Administrator by November 2018, as anticipated by the *CATA Working Group Report*.

Additionally, great progress has been made on standards and in deployment plans. There have been three standards delivered between May and August of this year: (1) Display Framework for Verified Caller ID; (2) APIs for Centralized Signing & Signature Validation Server; and (3) Management and Operational Considerations for STI-CAs and Policy Administrators. Carriers and others are deploying SHAKEN/STIR and a wide swath of the ecosystem has committed to implement these procedures and protocols.[38]

To the extent the FCC takes action, it should do so consistent with the recommendations in the *CATA Working Group Report*. Of note, one of the *CATA Working Group Report's* recommendations was "a safe harbor for unintended blocking or mis-identification of the level of trust for individual calls would provide a strong incentive for communications service provider adoption of SHAKEN, particularly where analytics are overlaid on the framework. Such liability protection may override reluctance to participate in SHAKEN, particularly in its early stages."[39] The *CATA Working Group Report* also recommended that the "FCC can also speed or promote more widespread adoption by incentivizing IP-to-IP interconnection for voice service providers because of the IP-to-IP connectivity required for the most fulsome level of attestation that can occur under the SHAKEN framework."[40] CTIA supports these recommendations.

2. Carriers and partners, including the app industry, have innovated to offer consumers numerous tools to identify and block unwanted, illegal calls.

[38] *See* Comments of CTIA, CG Docket No. 17-59, at 8-9 (July 20, 2018) (listing the commitments of 14 entities, including carriers and others in the ecosystem).
[39] *CATA Working Group Report* at 14.
[40] *Id.*

In addition to carrier-initiated blocking, consumer opt-in labeling and blocking services—offered by carriers and third parties—enable consumers to identify and block unwanted and illegal calls. While the *Public Notice* focuses on carrier-initiated call blocking, it rightly acknowledges these additional tools.[41] Some examples of these offerings include:

- **AT&T**—AT&T has rolled out a free, opt-in service called "Call Protect" to allow customers with certain iPhones[42] and HD Voice-enabled Android handsets to automatically block suspected fraud calls. As of June 28, 2018, AT&T has blocked more than 223 million fraud calls, and labeled more than 274 million spam calls, through AT&T Call Protect.[43] AT&T offers another opt-in service—Call Protect *Plus*—for a charge of $3.99 per month; this service offers the benefits of the Call Protect service, with additional features such as enhanced caller ID and reverse number lookup.[44]

- **Sprint—** Sprint partnered with Cequint to enhance its Premium Caller ID product that allows customers to subscribe to an optional, paid service that lets them receive information about the type of caller that is attempting to reach them and to set up preferences to send calls to voicemail or to block them entirely, category by category.

- **T-Mobile**—T-Mobile's Scam ID, which identifies calls that are likely to be fraudulent, is offered to all new T-Mobile and Metro PCS customers automatically. T-Mobile's Scam Block is offered to all customers on an opt-in basis. Both services are network-based and free of charge to customers.

- **U.S. Cellular**—U.S. Cellular is offering all Android and iOS customers a device application that offers free and premium robocall identification and blocking capabilities. The application—Call Guardian—protects customers by revealing the names of non-malicious callers who are not in the called party's contacts. The free subscription identifies incoming calls with the highest risk/toxicity scores for free. Alternatively, the premium subscription identifies callers of all risk levels, and offers the option to block calls based on the caller's identified risk level.

---

[41] *See Public Notice* at 3 ("There are numerous third-party applications that offer call blocking or labeling services directly to consumers. … we seek comment on the extent to which providers include access to these services as part of their own offerings.").
[42] Eligible iPhones include iPhone 6 or above running iOS v9.3+.
[43] *July 20, 2018 AT&T Comments* at 2-3 (explaining that these numbers are distinct from AT&T's carrier-initiated blocking statistics reported above).
[44] *See generally,* AT&T, Features – Security Apps, https://www.att.com/features/security-apps.html.

- **Verizon—** Verizon has deployed and continues to expand robocall mitigation features for wireless and wireline customers. For wireless, Verizon offers blocking and labeling services on most smartphones through its Caller Name ID service, which includes a spam filter that forwards to voicemail any calls corresponding to the spam risk level selected by the customer. This service includes a "risk meter" that classifies each incoming call and permits subscribers to either make their own decisions on whether to answer likely-unwanted calls, or to select the category/categories of calls that they want to be automatically filtered and sent to voicemail. And Verizon's Spam Alerts provide wireline customers who have Caller ID – whether they are on copper or fiber – with enhanced warnings about calls that meet Verizon's spam criteria by showing the term "SPAM?" before a caller's name on the Caller ID display.

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. App platforms saw a 495% increase in the number of available call blocking apps between October 2016 and March 2018.

The FCC should support these activities by establishing liability protection, perhaps in the form of a safe harbor, for carriers who offer such services or partner with third-party providers for the benefit of their customers. As with carrier-initiated blocking, carriers face liability risks when offering opt-in blocking and labeling services or partnering with third-party service providers. CTIA appreciates the Commission's prior strong support for carriers to offer these types of tools; in the *2015 TCPA Omnibus Order*, the Commission declared that "[n]othing 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."[45] The Commission should continue to prioritize consumer choice and empower consumers to "choose to use . . . technology to stop unwanted

[45] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Declaratory Ruling and Order, 30 FCC Rcd. 7961, ¶ 2 (July 10, 2015) ("*2015 TCPA Omnibus Order*").

calls" by establishing a safe harbor to protect well-meaning carriers from liability related to offering such tools.[46]

3. **The wireless industry is continuing its consumer education work.**

Consumer education is a critical tool in the fight against illegal robocalls. CTIA prioritizes consumer education and has updated its webpage devoted to increasing awareness of robocall prevention tools and providing consumers instructions on how to stop robocalls.[47] CTIA and its members have participated in federal agency outreach to consumers as well.[48] In addition, the FCC recently partnered with AARP "to educate older Americans about different kinds of phone scams," hosting Telephone Town Halls covering topics like how to avoid phone scams.[49] The Commission should continue these valuable consumer education efforts.

C. Industry Traceback Efforts Are Improving the Ability To Stop Bad Actors.

Because illegal robocalls will inevitably continue despite the extensive mitigation tools and efforts described above, carriers and others have been working to determine the *source*. Traceback, the process by which the origin of an illegal robocalling campaign is discovered, allows industry and law enforcement to identify and stop the cause of illegal robocalling activities.[50] Once the origin of an illegal campaign is traced, carriers can work to prevent those bad actors from using the carriers' networks and can refer cases to law enforcement. Coupling

---

[46] *Id.* ¶ 152.
[47] CTIA, *How to Stop Robocalls*, https://www.ctia.org/consumer-resources/how-to-stop-robocalls/.
[48] *See, e.g.*, Stop Illegal Robocalls Expo, FCC/FTC (April 23, 2018) https://www.ftc.gov/news-events/events-calendar/2018/04/stop-illegal-robocalls-expo-co-hosted-ftc-federal-communications
[49] P. Webre, *FCC & AARP Join Forces to Educate Older Americans about Phone Scams*, FCC Blog (Sept. 12, 2018), https://www.fcc.gov/news-events/blog/2018/09/12/fcc-aarp-join-forces-educate-older-americans-about-phone-scams.
[50] The *Public Notice* seeks to "refresh the record on industry traceback efforts." *Public Notice* at 3.

industry-level action with enforcement action may prove very productive, as tracebacks often point to a few bad actors.

Industry has taken a leading role in traceback. Industry participants have come together in the USTelecom Industry Trace Back ("ITB") Group to share information to more effectively trace back illegal robocalls. The ITB Group is focused on improving the speed of traceback, expanding traceback capacity, and expanding traceback information sharing. Better traceback helps industry police illegal robocalling and helps law enforcement. Further, carriers participate in the ATIS Service Provider Contact Directory ("SPCD") described in the *2016 Robocall Strike Force Report*. The SPCD facilitates service of subpoenas for illegal call traceback.[51]

The Commission may consider encouraging participation in voluntary traceback efforts and take steps to improve international traceback options.[52] As noted in the *2017 Robocall Strike Force Report*, "[u]nfortunately, while numerous providers have formally joined our traceback efforts, and many others cooperate in good faith in tracebacks, there are still upstream carriers who refuse to cooperate, which prevents carriers from tracing these malicious calling events back to the origin of the call."[53] Further, traceback options for calls originating overseas are limited. The FCC can address this limitation by encouraging overseas regulators to prioritize call authentication frameworks and adjust international norms.

D. All FCC Work on Illegal Robocall Mitigation Should Be Guided by the Principles of Regulatory Flexibility and Safe Harbors.

[51] *See Public Notice* at 3 ("Are there other coordinated traceback efforts, and if so, which providers are participating in them?").
[52] *See id.* at 3 (asking what the Commission can do to facilitate traceback efforts and "are there any concerns that the Commission could address to facilitate traceback?").
[53] *Industry Robocall Strike Force Report*, FCC, at 19 (Apr. 28, 2017) ("*2017 Robocall Strike Force Report*"), https://www.ustelecom.org/sites/default/files/documents/Ex%20Parte-Strike-Force-Report-2017-04-28-FINAL.pdf.

Any action that the Commission takes should be flexible and permissive. Industry-driven solutions will evolve, but heavy-handed regulatory action will stifle innovative activity.

The Commission should avoid mandates and instead encourage carriers to mitigate illegal robocalls. Mandates are unwise, as they are easily overcome by new, evolving technologies on both sides—industry working to protect the network and consumers, and bad actors working to game the system. Mandates also provide a roadmap for bad actors, which ultimately makes the network less secure. Accordingly, the Commission should refrain from prescriptive regulations mandating particular practices. The Commission can better encourage more aggressive carrier mitigation tactics by implementing robust safe harbors.

V. THE CONCERN THAT LEGAL ROBOCALLS WILL BE IMPROPERLY LABELED OR BLOCKED SHOULD NOT DRIVE THE COMMISSION TOWARD A PRESCRIPTIVE APPROACH.

The *Public Notice* asks about improper blocking, which it defines as blocking "for any reason other than to stop illegal calls."[54] This concern appears to drive the *Public Notice*'s discussion of "enforceable criteria"[55] and the discussion of white lists, un-blocking, and some form of alert to call originators that their calls have been blocked.[56]

Industry shares concerns about inadvertent erroneous blocking. Industry does not want to interfere with *legal* calling. As CTIA has made clear to the Commission in this proceeding, "[c]arriers share the FCC's longstanding priority of call completion and want to keep their customers satisfied" and "carriers have every incentive to address the claims of their customers who believe that their numbers are blocked in error."[57] Industry is collaborating and innovating

[54] *Public Notice* at 2.
[55] *See supra* Section III.B.
[56] *Public Notice* at 3-4.
[57] Comments of CTIA, CG Docket No. 17-59, at 3 (Jan. 23, 2018) ("*January 23, 2018 CTIA Comments*").

to prevent "false positives" and to ensure that legitimate callers do not get mistaken for illegal callers and inadvertently blocked. For example, "AT&T has established an ongoing and constructive dialogue with call originators to understand and, where valid, address concerns they have raised."[58] It also has "established procedures designed to ensure no legitimate traffic is impacted by its illegal robocall blocking program."[59] Further, industry has an ongoing dialog with the Professional Association for Customer Engagement (PACE).[60]

CTIA urges the Commission to better understand the many factors that may lead to false positives before taking any action. False positives in the carrier-initiated blocking context are different from false positives in the context of third-party blocking and labeling services and customer opt-in services. The record appears to conflate these scenarios; a claim cited in the *Public Notice* that there is "[a] current problem of overblocking" lumps together "voice service and call blocking/labeling providers."[61] False positives are distinct from consumers making informed decisions to decline calls using tools that have been made available by carriers and others. Industry is committed to reducing the risk of true false positives.

It is not reasonable to assume that reduced answer rates for legitimate robocalls is only or even primarily due to erroneous labeling or blocking. The trend of fewer consumers answering legitimate robocalls is likely associated with the increase in public awareness about robocalling tools and their use by consumers. If legitimate callers see a drop in call completion, then it may be because consumers are simply not picking up the phone. Rather than blame carriers and seek

[58] *See July 20, 2018 AT&T Comments* at 7 ("PACE has been a thoughtful and receptive partner with AT&T in this work.").
[59] *Id.* at 11.
[60] *See, e.g., id.* at 8.
[61] Sirius XM Radio Inc. Ex Parte, CG Docket No. 17-59 (June 7, 2018).

a regulatory solution, call originators should take steps to investigate and understand why their calls are not being answered and work with carriers to develop remedies.

CTIA urges the Commission to closely scrutinize troubling claims in the record regarding the reduction in call completion rates due to carrier-initiated blocking. Specifically, PACE has stated that

> "[c]arrier-based call blocking, while arguably an effective solution for blocking calls originating from numbers requested to be blocked by subscribers and invalid or unallocated/unassigned numbers, poses a high risk of blocking legal and legitimate communications if applied to presumptively illegal calls using ill-defined standards. PACE members experience the effects of call blocking every day, including, for some members, 20%- 30% reductions in call completion rates. . . . PACE is very concerned about carriers and mobile applications erroneously blocking legal and legitimate calls."[62]

Without further substantiation, CTIA questions whether, if any PACE members are indeed experiencing such call completion rate reductions, the reductions can be linked back to carrier-initiated blocking. The Commission should keep in mind that the carrier-initiated blocking it already permitted is quite limited. Carrier-initiated blocking under the *2017 Call Blocking Order* is limited to (1) calls purporting to originate from invalid numbers, (2) calls purporting to originate from numbers not allocated to any provider, and (3) calls purporting to originate from numbers that are allocated but unused.[63] This is unlikely to be the source of significant false positive errors. Indeed, the carrier-initiated blocking statistics from AT&T and T-Mobile cited above suggest that the modest blocking authorized by the FCC is not capable of having the sort of impact claimed by PACE.

---

[62] Comments of Professional Association for Customer Engagement, CG Docket No. 17-59, at 3-4 (Jan. 23, 2018).

[63] *See 2017 Call Blocking Order* ¶ 18. The *2017 Call Blocking Order* additionally authorized blocking at the request of the subscriber to an originating number. *Id.* ¶¶ 10-17.

Not only does the record lack evidence that false positives from carrier-blocking are a problem, but there is evidence to the contrary. AT&T reports that under its wholesale blocking program, it has only received unblocking requests in "very limited instances,"[64] and when wholesale customers have utilized AT&T's "bi-directional open lines of communication" and made an un-blocking request, AT&T aims to resolve the issue within 24 hours, although troubleshooting and resolving issues, in experience, has ranged from a few hours to a few days.[65] Generally, carriers address "unblocking" quickly when it is brought to their attention.

Accordingly, the Commission should reject calls for regulation. Specifically, the Commission should reject calls for un-blocking mandates and onerous reporting requirements for carriers. Such solutions are premature and unnecessary and would risk stifling innovation. These solutions would only address a small portion of current blocking activity.[66]

In addition, the Commission should reject calls for "white lists."[67] White lists are difficult to update, they present a target for hackers and security vulnerabilities, and they are fundamentally antithetical to federal telecommunications policy of open and seamless call completion.[68]

Finally, the Commission should reject calls to require providers to provide a real-time alert when calls are blocked.[69] Specifically, CTIA opposes PACE's proposal that the

---

[64] AT&T Ex Parte, CG Docket No. 17-59, at 2 (Sept. 22, 2017).
[65] *Id*.
[66] Moreover, customer opt-in services and third-party services should not be affected by this proceeding. *See generally January 23, 2018 CTIA Comments.*
[67] The *Public Notice* asks detailed questions about white lists. *Public Notice* at 3-4.
[68] *See* Comments of CTIA, CG Docket No. 17-59, at 7-8 (July 31, 2017).
[69] *See Public Notice* at 4 ("Are there other methods through which providers could reliably inform a caller that a call has been blocked?"); *See also,* Comments of Professional Association for Customer Engagement, CG Docket No. 17-59, at 4-6 (July 20, 2018) ("*July 20, 2018 PACE Comments*") ("PACE remains concerned about the lack of real-time blocking notification for callers.").

Commission require carriers to "alert callers and call recipients when calls are blocked."[70] Providing these alerts on a large scale raises CPNI issues and would be technologically unsound, as it would create massive network overhead and congestion. Additionally, the proposal to send consumer alerts when robocalls to their numbers are blocked—via push notification or text message, as suggested by PACE—runs completely counter to the goals of robocall abatement. Call blocking is meant to remove the annoyance to consumers of receiving unwanted robocalls; receiving a text message or a push notification that an unwanted robocall was blocked risks being just as problematic as the robocall itself. In any case, mandates for technological solutions like call blocking alerts are unwise and ineffective.[71] This is especially true in this case, where the "problem" being solved for is unclear. Further, with the development of new technologies, for example, caller registration and SHAKEN/STIR, this solution will be unnecessary. Rather than legitimate callers (such as PACE members) needing to rely on a real-time alert to know whether they have been blocked, they will be able to proactively work with carriers to register and to implement SHAKEN/STIR or to partner with the carriers to ensure signing of their calls.

VI. CONCLUSION.

CTIA appreciates the Commission's continued focus on the challenge of illegal robocalls. Industry is on the front lines of this fight, and carriers are embracing the Commission's permissive rules regarding carrier-initiated blocking, as well as other tools that are being developed and deployed at a rapid pace. The Commission should encourage carriers' aggressive

[70] *July 20, 2018 PACE Comments* at 6. PACE suggests that for caller blocking alerts, "the Commission could require use of a new signaling cause code specifically for calls blocked by carriers" and for consumer blocking alerts, "carriers could provide an optional push notification or free SMS message alerting the call recipient of the number blocked and providing instructions to remove the block." *Id.* at 5.

[71] While there could be scenarios where carriers voluntarily choose to provide such alerts, the Commission should not mandate these alerts.

and multi-pronged offensive against illegal robocallers by promoting flexibility and safe harbors. And it should avoid heavy-handed mandates that will stifle innovation and complicate consumer choice.

Respectfully submitted,

/s/ Krista L. Witanowski

Krista L. Witanowski
Assistant Vice President, Regulatory Affairs

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

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

www.ctia.org

September 24, 2018