Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
Consumer and Governmental Affairs Bureau Seeks Input for Report on Robocalling	)	DA 18-638

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

July 20, 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	)	CG Docket No. 17-59
Consumer and Governmental Affairs Bureau Seeks Input for Report on Robocalling	)	DA 18-638

COMMENTS OF CTIA

CTIA[1] respectfully submits these comments in response to the Federal Communications Commission's ("FCC" or "Commission") Consumer and Governmental Affairs Bureau's Public Notice ("*Public Notice*") seeking input for a staff report on robocalling mitigation efforts.[2]

I. INTRODUCTION AND SUMMARY.

Industry and the FCC are aggressively working to mitigate illegal robocalling, which is a challenge for the entire ecosystem. Solutions will require more than carrier action, but CTIA members are proud to be leading efforts to empower consumers and help fight illegal robocalls. Carriers are using network-based techniques, leveraging the proliferation of apps and other third-party tools, educating consumers, deploying call authentication technology, and collaborating

[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 Input for Report on Robocalling*, CG Docket No. 17-59, Public Notice, DA 18-638 (June 20, 2018) ("*Public Notice*").

with aggregators, innovators, and regulators. The ecosystem has seen tremendous growth in the capabilities that carriers and consumers have available to combat illegal robocalling.

The Commission deserves credit for helping to facilitate innovation and collaboration. The Commission has recognized the importance of consumer choice, affirming that "nothing in the Communications Act or our rules or orders prohibits carriers or VoIP providers from implementing call-blocking technology that can help consumers who choose to use such technology to stop unwanted robocalls."[3] This recognition of consumer choice in stopping unwanted robocalls, along with other FCC actions, has helped to facilitate innovation in the app space, paved the way for carriers to further enhance consumer choice, and led to a proliferation of activity, including industry driving emerging call authentication protocols and the FCC authorizing additional, limited blocking activity.

Amid this flurry of government and private sector activity, this *Public Notice* seeks information about what progress is being made. Efforts are promising, but with so much going on, it is premature to try to measure the effectiveness of these many activities. It is important to note that the Commission's *Call Blocking Order*,[4] which became effective February 12, 2018, is

---

[3] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 30 FCC Rcd. 7961, ¶ 152 (July 10, 2015) (internal citations omitted). It continued that "[c]onsumers currently have the choice to use call-blocking technology to block individual numbers or categories of numbers, and may continue to do so." *Id.*

[4] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order and FNPRM, 32 FCC Rcd. 9706 (Nov. 17, 2017) ("*Call Blocking Order*"). The FCC gave "voice service providers the option of blocking illegal robocalls in certain, well-defined circumstances," but wisely did not *mandate* call blocking of any kind. *Protecting Consumers and Businesses from Fraudulent Robocalls, Congressional Research Service Report*, at 14 (Jan. 5, 2018). As service providers evaluate various call blocking approaches, the Commission can create incentives for providers to make available innovative options by adopting a safe harbor from liability for providers who block calls as authorized by the Commission. The FCC declined to create a safe harbor for voluntary blocking, which CTIA urged it to adopt. *See* Comments of CTIA, WC Docket No. 17-97 (filed Aug. 14, 2017); Reply Comments of CTIA, WC Docket No.

still very new.[5] Additionally, industry, consumers, and other ecosystem participants are still deploying and evaluating tools, and some Commission and industry efforts are still being implemented. For example, the Commission recently delegated developing policy and implementation approaches to the North American Numbering Council's ("NANC") Call Authentication Trust Anchor Working Group ("CATA Working Group"). That process has been on the implementation track recently. Moreover, the threat landscape is evolving, revealing shifts in robocalling tactics in response to improved prevention efforts.

The Commission should support these ongoing efforts and continue to emphasize enforcement against bad actors. CTIA applauds the FCC and the Federal Trade Commission ("FTC") on recent high-profile enforcement actions. We encourage the agencies to continue pursuing illegal robocall schemes and to ensure that fines are paid, increasing the costs of illegal activity through a "whole of government" approach. Finally, the FCC and the FTC should lead internationally to change norms and evangelize call authentication protocols, which need to be deployed globally.

II. THE COMMUNICATIONS SECTOR HAS MADE STRIDES IN MITIGATING ILLEGAL ROBOCALLING, AND THERE IS MOMENTUM TO CONTINUE EMPOWERING CONSUMERS AND STOPPING HARMFUL CALLS.

A. The Industry Strike Force has galvanized efforts to fight robocalls.

Industry jump-started efforts to defeat the scourge of robocalls by establishing the Industry Robocall Strike Force in 2016. As the Commission has recognized, "[t]he Strike Force made significant progress toward arming consumers with call blocking tools and identifying

17-97 (filed Sept. 13, 2017). The FCC asserted that it did not have a sufficient record to act on the safe harbor. *Call Blocking Order* n.28. Without a safe harbor for authorized call blocking, carriers continue to face risks related to inadvertent blocking.

[5] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Final Rule, 83 Fed. Reg. 1566 (Jan. 12, 2018) (listing Feb. 12, 2018 as the effective date).

ways voice providers can proactively block illegal robocalls before they ever reach the consumer's phone,"[6] and the Strike Force was an impetus for the FCC's Call Blocking Order.[7] The Strike Force has prompted carriers to develop new technologies, improve data analytics, increase collaboration, and educate consumers. As recently reported in the *Wall Street Journal*: "Service providers have upped their robocall-protection offerings recently."[8] Among other things, the industry:

- Collectively blocks millions of robocalls per day.[9] Indeed, between October 2016 and June 2018, AT&T alone blocked 3.9 billion illegal calls from being delivered to customers. T-Mobile's Scam ID has resulted in more than 3 billion scam calls tagged since launch.
- Is adopting new call blocking and spam call prediction tools for customer use.[10]
- Continues to leverage the capabilities of the app industry. App platforms have seen a 495% increase in the number of available call blocking apps between October 2016 and March 2018. Carriers recognize that third-party robocall prevention apps can be effective and empowering for consumers.
- Continues to focus on consumer education. CTIA has updated its webpage devoted to increasing awareness of robocall prevention tools and providing consumers

[6] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Notice of Proposed Rulemaking and Notice of Inquiry, 32 FCC Rcd. 2306, ¶ 7 (Mar. 23, 2017), https://docs.fcc.gov/public/attachments/FCC-17-24A1_Rcd.pdf.

[7] *Call Blocking Order* ¶¶ 5-7 (noting that ("[t]he Strike Force specifically asked the Commission to provide guidance on when providers may block a call that the provider believes is illegal" and then "sought [additional] clarification that: (1) providers may block calls where the Caller ID shows an unassigned number; and (2) providers may block calls that the provider has determined to be illegal robocalls, so long as the provider takes reasonable steps to confirm that the calls are illegal").

[8] *See, e.g.*, Katherine Bindley, *Why Are There So Many Robocalls? Here's What You Can Do About Them*, Wall Street Journal (July 4, 2018), https://www.wsj.com/articles/why-there-are-so-many-robocalls-heres-what-you-can-do-about-them-1530610203?mod=searchresu lts&page=1&pos=1&ns=prod/accounts-wsj.

[9] CTIA Ex Parte Notice, CG Docket No. 17-59; WC Docket No. 17-97 (filed Jan. 23, 2018) ("*CTIA January 2018 Ex Parte*").

[10] *Id. See also infra* Section II.B.

instructions on how to stop robocalls.[11] CTIA and its members have participated in federal agency outreach to consumers as well.

- Is partnering with standards bodies like the Alliance for Telecommunications Industry Solutions, Inc. ("ATIS") IP-NNI Task Force and SIP Forum on the SHAKEN/STIR call authentication framework.[12]
- Assists the FTC and the FCC with law enforcement's investigations against robocallers and maintains relationships with call fraud bureaus that may initiate investigations after a suspected mass illegal robocalling event.[13]

B. Carriers and partners in the ecosystem—such as app developers—have created tools that empower consumers to block illegal robocalls.

Numerous tools are available to help consumers identify and block illegal robocalls.[14]

Many of these tools are free. Some examples of carriers' offerings include:

- **AT&T**—AT&T rolled out a service called 'Call Protect' to allow customers with iPhones and HD Voice enabled Android handsets to automatically block suspected fraud calls. In addition, AT&T offers AT&T Digital Call Protect for IP wireline phones.
- **Sprint—**Sprint has partnered with Cequint to enhance its Premium Caller ID product that allows customers to subscribe to an optional, paid service that empowers them to receive information about the type of caller that is attempting to reach them and to set up preferences to send those calls to voicemail or to block them entirely, category by category.
- **T-Mobile**—T-Mobile's Scam ID and Scam Block are automatic, network-based services offered free of charge that allow customers to immediately see when calls come in from likely scammers, and to block all likely scammers before they reach the consumer. These tools were rolled out in March 2017 to address the growing problem of fraudulent and unwanted calls. T-Mobile also has DNO blocking, both on its network and within the PrivacyStar solution.
- **U.S. Cellular**—U.S. Cellular is currently offering all Android and iOS customers a device application that offers free and premium robocall identification and blocking capabilities. The application—Call Guardian—protects U.S. Cellular customers by revealing the names of non-malicious callers who are not in the called party's

[11] CTIA, *How to Stop Robocalls*, https://www.ctia.org/consumer-resources/how-to-stop-robocalls/.

[12] *CTIA January 2018 Ex Parte*.

[13] *Id.*

[14] The *Public Notice* asks for information about the "opt-in tools that enable consumers to identify and block illegal calls." *Public Notice,* at 2.

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 subscriber the option to block calls based on the caller's identified risk level.

- **Verizon—** Verizon has deployed and continues to expand robocall mitigation features as part of its Caller Name ID service, including a spam filter that forwards to voicemail any calls corresponding to the spam risk level selected by the customer. 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.

Additionally, data analytics providers are developing an array of sophisticated analytics engines that help subscribing carriers and customers to identify calls that are likely to be illegal or unwanted.

It is too early to determine these tools' efficacy, but it is clear that consumers are growing savvier and are seeing new tools become available at a rapid pace.

C. SHAKEN/STIR and related developments represent the next generation of anti-robocall measures.

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. These protocols will enable "verif[ication] and authenticat[ion] [of] caller identification for calls carried over an Internet Protocol (IP) network."[15] As the Commission has explained, there are three phases associated with SHAKEN/STIR:

> Phase 1 consists of development of the SHAKEN framework, based on the protocols developed by the IETF's STIR working group (the STIR framework), and describes the operations necessary for making an authenticated telephone call

[15] *Robocall Strike Force Report*, at 3 (Oct. 26, 2016).

> using the SHAKEN framework. Phase 2 consists of the "Governance Model and Certificate Management for the Trust Anchor," describing the way in which entities will be granted the trust necessary to vouch for call authenticity, and the organizational structures needed to manage this process. Phase 3 consists of the "Call Validation Display Framework" that will recommend how to display SHAKEN/STIR information to consumers. Phase 3 is still being developed by ATIS and the SIP Forum . . . .[16]

"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."[17] As one of Chairman Pai's advisors told the NANC, this "call authentication work" by the diverse private sector participants in the CATA Working Group "is really one of the key pillars into this overall effort" to help reduce illegal robocalling.[18]

Currently, SHAKEN/STIR is in Phase 2. 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.[19] Chairman Pai promptly accepted these recommendations.[20] There has been significant progress on the call authentication trust anchor, even in the short time since the *CATA Working Group Report* was issued. Pursuant to Section 3 of that report, industry stakeholders from the trade associations noted in the report agreed that the

---

[16] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Inquiry, 32 FCC Rcd. 5988, ¶ 5 (July 14, 2017).

[17] *Robocall Strike Force Report*, at 3 (Oct. 26, 2016).

[18] North American Numbering Council Meeting Transcript (Final) (Apr. 27, 2018), https://docs.fcc.gov/public/attachments/DOC-351087A1.pdf.

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

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

Governance Authority should be set up under the auspices of ATIS. ATIS has agreed to lead the Governance Authority and Governance Authority Board, and is in the process of finalizing its proposed budget and budget allocation methodology; board make-up; corporate structure; and operating procedures. Per the *CATA Working Group Report*, ATIS is on target to announce the Governance Authority and its Board in August—just three months from submission of *CATA Working Group Report*.

Additionally, carriers and others in the ecosystem are deploying SHAKEN/STIR and a wide swath of the ecosystem has publicly committed to implementation.

- AT&T "plans to implement SHAKEN/STIR in parallel with the industry timeline for establishing the SHAKEN/STIR governance structure. AT&T plans to conduct further testing in 2018 and begin a general rollout in 2019."[21]
- Sprint "supports the adoption of SHAKEN/STIR call authentication by carriers but caution[s] that there are logistical obstacles to immediate deployment and that even when it is deployed, it will not be an immediate silver bullet that will eliminate illegal robocalls."[22]
- T-Mobile "plan[s] to commercially launch [its] STIR/SHAKEN network solution prior to the end of 2018. Also, [it] expect[s] that by the end of 2019, all handset specifications will include the requirements necessary to support display of the STIR/SHAKEN verification result."[23]
- U.S. Cellular has told the Commission that "[b]ased upon [its] current discussions with the vendor community and other carriers, [it is] tentatively planning to deploy a solution during the second half of 2019."[24]
- Verizon "expect[s] to achieve initial operational capability later [in 2018], with the bulk of production anticipated for 2019."[25]
- Bandwidth has discussed its implementation plan with the Commission.[26]

[21] AT&T Ex Parte Notice, CG Docket No. 17-59 (filed May 16, 2018).

[22] Sprint Ex Parte Notice, CG Docket No. 17-59 (filed May 15, 2018).

[23] T-Mobile Ex Parte Notice, CG Docket No. 17-59 (filed May 24, 2018).

[24] U.S. Cellular Ex Parte Notice, WC Docket No. 17-97 (filed June 22, 2018).

[25] Verizon Ex Parte Notice, CG Docket No. 17-59 (filed May 7, 2018).

[26] Bandwidth Ex Parte Notice, CG Docket No. 17-59 (filed May 25, 2018).

- "Nokia also is working to incorporate the latest technologies into our products to combat unwelcome robocalls and spoofed calls, by following the SHAKEN/STIR standards, to be available for commercial deployment in 2019. . . . [SHAKEN/STIR] is a whole-industry effort, and Nokia is working hard to meet the demands of our service-provider customers who are keenly interested in deploying these tools in their networks to provide the best experience possible for consumers."[27]

- CenturyLink predicts that consumer benefit impacts will be "visible beginning in 2019."[28]
- Charter has met with Commission staff to discuss "its ongoing commitment to protect its customers from illegal robocalling and spoofing, and its continued involvement in the development of industry standards for the SHAKEN/STIR framework . . . [and] its plans for implementing SHAKEN/STIR. . . ."[29]
- Cisco "ha[s] a roadmap for development of technology supporting STIR, that includes a trajectory for the delivery of capabilities in the 2019-2020 timeframe."[30]
- Comcast "plan[s] to conduct trials prior to the end of 2018 and scale to fuller implementation during 2019."[31]
- Cox's "target date to begin to test SHAKEN/STIR for its residential customers is late 2018 to early 2019 with broader implementation occurring in 2019."[32]
- Frontier has explained to the Commission "that it ha[s] already tested one SHAKEN/STIR solution and that it continues to evaluate the best strategy and roadmap to target and reduce robocalls in a way that makes sense for its customers as it moves forward with its network plans."[33]
- Google stated that it intends to implement SHAKEN/STIR.[34]

[27] Nokia Ex Parte Notice, WC Docket No. 17-97 (filed June 29, 2018).

[28] Century Link Ex Parte Notice, CG Docket No. 17-59 (filed May 24, 2018).

[29] Charter Ex Parte Notice, WC Docket No. 17-97 (filed June 4, 2018).

[30] Cisco Ex Parte Notice, CG Docket No. 17-59 (filed July 2, 2018).

[31] Comcast Ex Parte Notice, WC Docket No. 17-97 (filed May 18, 2018).

[32] Cox Ex Parte Notice, CG Docket No. 17-59 (filed May 23, 2018).

[33] Frontier Ex Parte Notice, CG Docket No. 17-59 (filed June 26, 2018).

[34] Google Ex Parte Notice, WC Docket No. 17-97 (filed June 1, 2018).

D. Industry is fully committed to consumer education, which is a powerful tool to mitigate illegal robocalls.

One of the strongest tools to mitigate illegal robocalls is consumer education.[35] There is an abundance of resources for consumers wishing to learn more about mitigating illegal robocalls. Industry is leading the way in making these resources available to consumers. CTIA, AT&T, Sprint, T-Mobile, U.S. Cellular, Verizon, and ACT—The App Association are just a few examples of carriers and industry groups that provide online resources for consumers regarding robocalls. Indeed, CTIA is a leading source of consumer education resources. According to the April 2017 Strike Force Report, "CTIA's consumer education efforts have been robust and effective."[36] CTIA's consumer resources webpage entitled *How To Stop Robocalls* provides consumer tips and a comprehensive list of over 550 mitigation apps, many of which are free, along with step-by-step video instructions for blocking calls on Android, BlackBerry, iOS and Windows devices.[37] Carriers continue to refer customers to this tool to guide them to the ever-growing variety of available third-party apps. In addition, CTIA uses social media to heighten public awareness about robocall mitigation. CTIA also has facilitated members' efforts to keep their consumer-facing content current in collaboration with Industry Strike Force initiatives.

[35] The FCC asks about "the progress made by industry, government, and consumers in combatting illegal robocalls." *Public Notice*, at 1.

[36] Robocall Strike Force Report, at 12 (Apr. 28, 2017).

[37] CTIA, *How to Stop Robocalls*, https://www.ctia.org/consumer-resources/how-to-stop-robocalls/.

III. AGGRESSIVE WORK ON ILLEGAL ROBOCALL MITIGATION IS IN ITS EARLY STAGES, MAKING MEASURING EFFECTIVENESS PREMATURE AND DIFFICULT.

A. Industry faces challenges in measuring the effectiveness of new solutions in a fluid and diverse ecosystem.

CTIA appreciates the FCC's interest in assessing how the concerted efforts of government and industry are playing out in the marketplace, but many efforts remain in their early stages. Ecosystem participants are evaluating the effectiveness of tools, and it is too soon to know how various efforts will impact illegal robocalling. For example, at the end of 2017 and early 2018, carriers started increasing call blocking, and we have seen 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."[38] This shows the fluidity of the robocalling landscape and how one remediation effort may lead illegal callers to adjust their tactics. Other tools are developing to combat neighbor spoofing. Call authentication, discussed above, is one such tool. Extracting data or discernible trends from a moment in time—particularly this early—would not be useful.

Additionally, the data sought in the *Public Notice* are not readily available and the resources to compile that data would be diverted from mitigation efforts. As CTIA has explained, reliable data about robocall volume and mitigation may be difficult to obtain because many entities (carriers, aggregators, and those offering call blocking services) collect information in various ways. Accordingly, data may be incomplete or not comparable. For example, carriers may not be able to determine call origination, because terminating carriers often receive traffic from intermediate and transit carriers who may not determine

[38] *See Spoofing and Caller ID*, FCC Consumer Guide, https://www.fcc.gov/consumers/guides/spoofing-and-caller-id (last updated July 5, 2018).

domestic/foreign origination. Further, carriers cannot respond to the FCC's inquiry regarding the "type of scam (IRS, grandparent scam, etc.)," as call content is not something carriers review or assess.

B. The FCC should be cautious about the reliability and relevance of data on robocall volume.

The *Public Notice* asks about existing complaint data,[39] but the data collected and made available by the government has significant limitations. The FCC's Consumer Complaint Data Center ("Data Center") provides informative data that can be used for some purposes or combined with other data sets. However, the Commission should not rely on this data as a benchmark for evaluating the effectiveness of FCC and industry efforts.

First, the FCC's Data Center does not adequately differentiate between illegal robocalls and legitimate calls. Automated calls are not by default illegal. The Telephone Consumer Protection Act ("TCPA") allows for automated calling pursuant to the regulatory framework, and the FCC has made clear that there are "a variety of legitimate reasons for altering caller ID information" that should not be treated the same as "malicious caller ID spoofing."[40] Complaints may relate to automated calls that are not illegal, including calls for which consent has been provided or which are not subject to the TCPA because an exception is available, or where caller ID information has been altered for a legitimate reason.[41] For example, automated political, charitable, debt collection, survey, and other informational and non-telemarketing calls to wireless numbers are generally permissible so long as the called party has given prior express

[39] *Public Notice*, at 2.

[40] *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Report and Order, 26 FCC Rcd. 9114, at ¶¶ 9, 40 (June 22, 2011).

[41] *See id.* (describing beneficial Caller ID manipulation on the part of domestic violence shelters and medical providers).

consent, and automated telemarketing calls are permissible with prior express written consent. Many consumers may find these types of calls unwanted and aggravating but it would be inaccurate to describe these calls as illegal and, indeed, carriers have no basis to block calls due to their annoying or aggravating content. Treating every reported robocall as illegal is methodologically unsound.

Second, Data Center data is crowd-sourced and the complaint entry process for the Data Center is not intuitive, especially compared to that of the FTC. *Third,* the Data Center has few requirements for uniform data entry, including the use of open text fields, which results in inconsistent, multiple, or inadvertent submissions. For all these reasons, Data Center data should not be used as the basis of FCC analysis of progress on illegal robocalling.

While the FTC uses more uniform data entry, its complaint database is also crowd-sourced and the information collected suffers from similar shortcomings: inconsistent, multiple or mistaken submissions, such as where a protected category of call may be tagged as an illegal robocall. The FTC complaint form lists several categories of calls that are in fact legally permissible. Accordingly, the FCC should be cautious before relying on this dataset as well.

IV. THE COMMISSION SHOULD CONTINUE TO CRACKDOWN ON ILLEGAL ROBOCALLING, PARTNER WITH OTHER AGENCIES, AND TAKE THE LEAD IN THE GLOBAL FIGHT AGAINST ROBOCALLS.

A. CTIA applauds the FCC and FTC for recent notable actions, including enforcement actions.

The *Public Notice* asks about the "challenges that remain in combatting illegal robocalls."[42] A fundamental challenge is that illegal robocalling is perpetuated by bad actors operating domestically and internationally. These bad actors are already violating federal law

[42] *Public Notice,* at 2.

and regulations. A combination of technological solutions and strong enforcement is key to mitigating this illegal activity.

The *Public Notice* also asks about enforcement.[43] CTIA applauds the FCC and the FTC on recent significant enforcement actions and encourages those agencies to continue pursuing illegal robocall schemes. Most recently, the FTC brought an enforcement action "to stop two related operations and their principals who allegedly facilitated billions of illegal robocalls to consumers nationwide, pitching everything from auto warranties to home security systems and supposed debt-relief services."[44] The FTC reports staggering robocall figures originating from these bad actors: from January 2014 to May 2016, 883 million average unlawful robocalls per year, with an average of 157 million of these connected to numbers on the Do Not Call Registry; and from January 2016 – May 2016, 54 million connected calls used spoofed caller ID numbers. In that short time (January to May 2016), these calls generated 8,000 FTC consumer complaints.[45]

The FCC has engaged in high-profile enforcement actions as well. It issued a $120 million fine against Adrian Abramovich, who ran a "massive robocalling operation aimed at selling timeshares and other travel packages."[46] The operation made close to 100 million spoofed robocalls over three months, in violation of the Truth in Caller ID Act.[47] The

---

[43] *Id.* ("How are law enforcement authorities proceeding against robocallers and what has been the effect of those efforts?").

[44] *FTC Sues to Stop Two Operations Responsible for Making Billions of Illegal Robocalls,* FTC (June 5, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-sues-stop-two-operations-responsible-making-billions-illegal.

[45] *Id.*

[46] *FCC Fines Massive Neighbor Spoofing Robocall Operation $120 Million,* FCC (May 10, 2018), https://docs.fcc.gov/public/attachments/DOC-350645A1.pdf.

[47] *Id.*

Commission should not let the fine go unpaid. If Mr. Abramovich does not pay the forfeiture, the FCC should refer his case to the Department of Justice to serve as a deterrent to bad actors who place such calls in flagrant disregard for federal law.

In addition, the FCC and FTC are collaborating on awareness and innovation. On March 23, 2018, the agencies hosted a Joint Policy Forum on Illegal Robocalls[48] and on April 23, 2018, they hosted a Stop Illegal Robocalls Expo, to offer a "platform for showcasing innovative technologies, devices and applications that will improve consumers' daily lives by combatting illegal robocalls," and included a discussion on robust and focused enforcement.[49]

B. The Commission should collaborate with carriers and other federal agencies in a "whole of government" approach, and should lead internationally to thwart illegal operations.

Collaboration with carriers and other agencies can yield significant relief. This is illustrated by the FCC's Enforcement Bureau's work with the FTC and the Treasury Inspector General for Tax Administration ("TIGTA") in 2016 to block the illegal robocallers behind the prolific IRS scam calls. Ultimately, this collaboration led to the indictment of 56 individuals behind the massive scam that resulted in 1.8 million people reporting that they had received an impersonation call and more than 9,600 victims reporting that they had paid these criminals a total amount of more than $50 million dollars.[50] "[A]ccording to the Better Business Bureau's

---

[48] *FTC and FCC to Host Joint Policy Forum on Illegal Robocalls*, FTC Media Advisory (Mar. 22, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-host-joint-policy-forum-illegal-robocalls. *See also Fighting the Scourge of Illegal Robocalls* (Mar. 23, 2018), https://www.fcc.gov/fcc-ftc-robocalls-forum.

[49] *Stop Illegal Robocalls Expo* (Apr. 23, 2018), https://www.fcc.gov/news-events/events/2018/04/stop-illegal-robocalls-expo.

[50] *Inspector General Comments on Indictment of Alleged IRS Phone Fraud Scammers*, Treasury Inspector General for Tax Administration (Oct. 27, 2016), https://www.treasury.gov/tigta/press/press_tigta-2016-31.htm; Charles Riley & Omar Khan, *India busts bogus call centers for posing as the IRS*, CNN Money (Oct. 6, 2016), http://money.cnn.com/2016/10/06/news/india-irs-scam-

Scam Tracker, the numbers of IRS-related scam complaints have dropped dramatically" since this enforcement action.[51]

Traceback efforts are another example of the benefits of public-private collaboration.[52] Carriers have worked with the USTelecom Industry Trace Back ("ITB") Group to conduct investigations of robocalls and have presented traceback information to investigating authorities. Further, carriers participate in the ATIS Service Provider Contact Directory ("SPCD") developed by the October 2016 Strike Force Report. The purpose of the SPCD to facilitate service of subpoenas for illegal call traceback.

A comprehensive approach across the federal and state governments is essential.[53] U.S. Attorneys' offices nationwide can prioritize enforcement where federal statutes, such as the Truth in Caller ID Act, are violated in furtherance of a fraud or other malicious action. They can partner in enforcement at the state level, and work with the FCC, FTC, and international partners on enforcement cases, particularly when the calls originate outside of the United States. A

---

arrests/.

[51] Kelly Phillips Erb, *Bogus IRS Calls Topped List of Most Reported Scams in 2016*, Forbes (Jan. 8, 2017), https://www.forbes.com/sites/kellyphillipserb/2017/01/08/bogus-irs-calls-topped-list-of-most-reported-scams-in-2016/#7e611b432076.

[52] *Public Notice*, at 2 ("How is traceback making a difference in enforcement against unlawful robocalls?").

[53] Other widespread criminal activity has benefitted from a "whole of government" approach that addressed the roles of bad actors, consumers, and legitimate businesses. *See, e.g.*, Mortgage Fraud, United States Department of Justice Executive Office for United States Attorneys, The United States Attorneys' Bulletin, Vol. 58, No. 3, at 1-2, (May 2010), https://www.justice.gov/sites/default/files/usao/legacy/2010/05/27/usab5803.pdf (describing the comprehensive approach taken to address mortgage fraud); *Combating Identity Theft: A Strategic Plan*, The President's Identity Theft Task Force, at 7-9 (Apr. 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (describing the approach to identity theft).

comprehensive approach is essential to address the source of robocalls because there are recidivist bad actors who do not care about breaking the law and quickly change tactics.

Some illegal operations warrant criminal enforcement, and the FCC and FTC should work with DOJ to bring appropriate criminal prosecutions under the wire fraud law. Criminal enforcement is not appropriate for all activity related to automated calling, but can be an important deterrent to the fraud and abuse perpetrated using illegal robocalls.

Finally, without international cooperation, better authentication and filtering may have the unintended result of additional bad actors moving off-shore. The FCC needs to lead overseas to change norms and evangelize call authentication protocols. The *Public Notice* seeks information regarding "traceback options . . . for calls originating overseas."[54] Traceback options for calls originating overseas are limited at present. The FCC can address this limitation by encouraging overseas regulators to prioritize call authentication frameworks and adjust international norms. And as industry experts have explained, as authentication protocols are adopted in the United States, there "is a continuing risk" that "[t]he bad guys may begin to shift more of their call originations overseas to countries that don't work with the U.S. on STIR/SHAKEN."[55]

V. CONCLUSION.

CTIA and its members share the Commission's commitment to address illegal robocalling. While industry and government efforts have yielded positive results for consumers, and new tools and services have empowered consumers and carriers to identify and block illegal robocalls, it is too early to fully assess the impact of these efforts. CTIA strongly encourages the

[54] *Public Notice*, at 2.

[55] North American Numbering Council Meeting Transcript (Final) (Apr. 27, 2018), https://docs.fcc.gov/public/attachments/DOC-351087A1.pdf.

Commission to continue its concerted effort to fight robocalls by redoubling its enforcement and collection activities to send a strong message to bad actors, and serving as a leader abroad to encourage other countries to adopt strong call authentication frameworks, target illegal actors, and otherwise adjust international norms.

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

July 20, 2018