

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

In the Matter of)
)
Protecting Consumers from One-Ring Scams) CG Docket No. 20-93

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

June 19, 2020

I. INTRODUCTION AND EXECUTIVE SUMMARY.

The wireless industry is dedicated to combatting one-ring scams and other harmful robocalls, consistent with the Commission’s top consumer protection priority and the directives in the bipartisan TRACED Act.¹ As the Commission knows, illegal robocallers continue to change their tactics to defraud or scam consumers—one-ring scams are just one type of fraudulent robocall scheme where scammers defraud consumers by tricking them into calling scammers back.² Given the constantly evolving problem of illegal and unwanted robocalls, the Commission has given providers many tools to protect consumers, such as blocking and labeling calls based on reasonable analytics, implementing call authentication solutions like STIR/SHAKEN, and other actions.³ Wireless voice service providers and their robocall mitigation partners have taken up this authority to protect consumers from *tens of billions* of illegal and unwanted robocalls, including one-ring scams.⁴

In order to ensure that voice service providers have certainty to use all available tools to protect consumers from harmful calls, the Commission should encourage continued blocking of illegal calls and the development of best practices to combat one-ring scams and other illegal and

¹ See *In the Matter of Protecting Consumers from One-Ring Scams*, Notice of Proposed Rulemaking, CG Docket No. 20-93, FCC 20-57, ¶ 2 (rel. Apr. 28, 2020) (“*One-Ring Scams NPRM*”) (“The Commission’s top consumer protection priority is stopping illegal calls.”); Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019) (“TRACED Act”).

² See, e.g., FCC, Consumer Guides, ‘*One Ring*’ Phone Scam, <https://www.fcc.gov/consumers/guides/one-ring-phone-scam> (last visited June 15, 2020) (“For illegal robocallers, the goal isn’t always getting you to answer. Sometimes, it’s getting you to call back”).

³ See, e.g., *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51, n.53 (rel. June 7, 2019) (“*2019 Call Blocking Declaratory Ruling*”); See *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706, ¶ 60 (2017) (“*2017 Call Blocking Order*”); *Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, Report and Order and Further Notice of Proposed Rulemaking, WC Docket Nos. 17-97, 20-67 (rel. Mar. 31, 2020).

⁴ See Comments of CTIA, CG Docket No. 17-59, WC Docket No. 17-97, at 6-7 (filed Jan. 29, 2020).

unwanted robocalls. The Commission should also adopt a broader safe harbor than the one proposed in the Commission's *NPRM* to further encourage providers to use all available tools to prevent one-ring scams and other illegal robocall schemes from defrauding consumers.

Specifically, the Commission should adopt a safe harbor that mitigates liability for providers' good faith efforts to block, label, or attest to calls based on reasonable analytics. By adopting these proposals, the Commission will build upon years-long efforts to combat one-ring scams by giving voice service providers more certainty, and incenting voice service providers to use all available tools to enhance the multi-pronged fight against illegal and unwanted robocalls.

II. THE COMMISSION SHOULD ENCOURAGE VOICE SERVICE PROVIDERS' EFFORTS TO PROTECT CONSUMERS FROM ONE-RING SCAMS.

CTIA supports the Commission's efforts to "encourage voice service providers to block one-ring scams," and urges 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.⁵ In so doing, the Commission need not adopt a new rule or grant of authority as proposed in its *NPRM*.⁶

As part of the multi-pronged fight against illegal and unwanted robocalls, voice service providers have been protecting consumers from one-ring scams and other fraudulent robocall schemes for years. One-ring scams are a well-known type of scam that prompted approximately 2,600 consumer complaints last year alone.⁷ One-ring scammers typically call consumers in the United States using a premium rate international phone number that may appear to come from a variety of callers, including a well-known U.S. business, spoofed domestic or international phone

⁵ *One-Ring Scams NPRM* ¶ 4.

⁶ See *One-Ring Scams NPRM* ¶ 14 (proposing to adopt rule allowing blocking of one-ring scam calls).

⁷ *One-Ring Scams NPRM* ¶ 4 (citing FCC consumer complaint data).

number, or simply “unknown caller” or “no caller ID.”⁸ The caller then hangs up after one ring (sometimes repeatedly), enticing the consumer to call the number back.⁹ Often the scammer places the consumer on an extended hold, resulting in high international toll charges, which are largely paid to the scammer.¹⁰ Leveraging reasonable analytics and their fraud prevention teams, voice service providers constantly monitor their networks to detect and block one-ring scams and other fraudulent traffic, as well as return calls to one-ring scammers.¹¹

Voice service providers have broad authority to block illegal calls, including one-ring scam calls, and they can, and do, lawfully block illegal one-ring schemes to protect consumers.¹² This broad, flexible authority to block illegal calls extends to blocking inbound, one-ring scam calls and to outbound calls where consumers are tricked into calling back numbers associated with such scams. In both cases, the blocking is performed to protect consumers from illegal calls, which is the Commission’s top consumer protection priority. While providers, the

⁸ See ‘One Ring’ Phone Scam, FCC, Consumer Guides, <https://www.fcc.gov/consumers/guides/one-ring-phone-scam> (May 2019); Colleen Tressler, “One-Ring Cell Phone Scam Can Ding Your Wallet, FTC Blog (Feb. 10, 2014), <https://www.consumer.ftc.gov/blog/2014/02/one-ring-cell-phone-scam-can-ding-your-wallet>.

⁹ *Id.*

¹⁰ *Id.*

¹¹ See, e.g., Letter from Christopher Oatway, Verizon, to Patrick G. Webre, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (Feb. 28, 2020) (“Customers also have the ability to block all incoming international calls, protecting them against scams like the Wangiri “one ring” scam.”); *Robocalls and Unwanted Calls*, AT&T CyberAware, <https://about.att.com/pages/cyberaware/ae/robocall> (explaining “unsolicited calls to phones where the receiving party may have to pay for the call are also illegal” and “AT&T offers customers services which can help identify a call that uses a spoofed telephone number as spam, fraud or neither, and blocks or flags the call accordingly”) (last visited June 16, 2020).

¹² For example, in the 2019 Call Blocking Declaratory Ruling, the Commission explained 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.” *2019 Call Blocking Declaratory Ruling*, ¶ 23 n.53; see also Comments of AT&T, CG Docket No. 17-59; WC Docket No. 17-97, at 15-16 (filed July 24, 2019) (explaining that “call completion rules do not apply to *illegal* calls”) (emphasis in original).

Commission, and other agencies have been protecting consumers from these scams for years, fraudsters continue to find new victims.¹³

The Commission should also encourage continued blocking of illegal calls and development of voluntary best practices to protect consumers from one-ring scams and other illegal and unwanted robocalls. For example, voice services providers have applied best practices to protect consumers from one-ring scams, including using reasonable analytics to identify and block incoming traffic from numbers associated with one-ring scams, alerting customers that international tolls may apply before they call back a number associated with a suspected one-ring scam, and blocking consumers' calls to known one-ring scam numbers, among other reasonable approaches. While encouraging continued blocking of illegal calls and voluntary adoption of evolving industry best practices will promote continued action to protect consumers from scammers, a broad safe harbor would further encourage providers to use all available tools to swiftly and effectively block one-ring scams and other ever-changing robocall schemes.

III. ADOPTING A BROAD SAFE HARBOR WOULD ENSURE THAT PROVIDERS HAVE CERTAINTY TO PROTECT CONSUMERS FROM ONE-RING SCAMS AND OTHER ABUSIVE ROBOCALLER TACTICS.

While wireless providers have been protecting consumers from one-ring scams for years, additional regulatory certainty can further incentivize providers to move quickly and effectively to combat these and other abusive robocalls. The Commission asks whether it should “consider a

¹³ See, e.g., *Alerts and Reporting: One-Ring Call Scams*, AT&T CyberAware, <https://about.att.com/pages/cyberaware/ar/wangiri> (last visited June 12, 2020); Colleen Tressler, “One-Ring” Cell Phone Scam Can Ding Your Wallet, FTC Blog (Feb. 10, 2014), <https://www.consumer.ftc.gov/blog/2014/02/one-ring-cell-phone-scam-can-ding-your-wallet>; *What Is a ‘One-Ring’ Scam?*, Snopes (Oct. 25, 2012), <https://www.snopes.com/fact-check/one-ring-scam/>; Aarti Shahani, *Why Phone Fraud Starts With a Silent Call*, NPR: All Tech Considered (Aug. 24, 2015), <https://www.npr.org/sections/alltechconsidered/2015/08/24/434313813/why-phone-fraud-starts-with-a-silent-call>.

one-ring specific safe harbor” and “how would any such safe harbor relate to any broader robocall-blocking safe harbor we may also adopt?”¹⁴ CTIA supports the Commission’s goals to help “facilitate blocking of one-ring scams” and “encourage voice service providers to block one-ring scams.”¹⁵ However, adopting a narrow safe harbor that is limited to a small category of fraudulent robocalls as the Commission proposes would not achieve this goal. Adopting a broader robocall-blocking safe harbor would more effectively help providers protect consumers from one-ring scams and many other types of abusive robocalls.

The Commission should adopt a broad safe harbor that mitigates liability for blocking, labeling, and trust identification decisions based on reasonable analytics, which may include STIR/SHAKEN data, to more effectively encourage blocking of one-ring scams and to achieve its broader priority to protect consumers from illegal and unwanted robocalls.¹⁶ The Commission is already considering a safe harbor for blocking certain robocalls more generally, as it notes, and already recognized that “adopting a safe harbor would greatly facilitate [provider call blocking] effort[s] *by providing carriers with more certainty.*”¹⁷ The Commission is right

¹⁴ ¶ 17 (emphasis added) (proposing a safe harbor that “could, for example, provide protection from liability under the Communications Act to voice service providers that in good faith block a call from a number (incorrectly thought to perpetuate a one-ring scam”).

¹⁵ ¶¶ 15, 17.

¹⁶ See Letter from Patrick Halley, USTelecom – The Broadband Association, Matt Gerst, CTIA, Steve Morris, NCTA, to Marlene H. Dortch, FCC, CG Docket No. 17-59, WC Docket No. 17.97, at 6 (filed Jan. 31, 2020) (proposing that the Commission deem in compliance with the Communications Act of 1934 and the Commission’s rules and not liable in any enforcement action or adjudicative proceeding a voice service provider that unintentionally or inadvertently blocked, mislabeled, or misidentified the level of trust for a call if at the time of the call the provider: i) took one or more reasonable action(s) including but not limited to: performing research on the phone number to reasonably determine the call was highly likely to be an illegal robocall; implementing reasonable procedures to block calls consistent with the Commission’s rules; or using reasonable analytics, which may include information provided by call authentication frameworks; ii) had procedures in place for blocking, labeling, or identification that were reasonably likely to confirm that calls blocked, labeled, or identified were limited to illegal or unwanted robocalls and the provider followed these procedures; iii) had procedures in place to address reported incidents of unintentional or inadvertent blocking, mislabeling, or misidentification of such calls; and iv) made reasonable efforts to avoid blocking, mislabeling, or misidentifying emergency public safety calls).

¹⁷ *2019 Call Blocking Declaratory Ruling* ¶ 59 (emphasis added); *id.* ¶¶ 24–25 (issuing the “declaratory ruling to resolve uncertainty and make clear the call-blocking tools that voice service providers can offer their customers”

that adopting a broad safe harbor will give providers more certainty, more strongly encouraging blocking of one-ring scams and other illegal and unwanted robocalls. By promoting providers' ability to use all available tools to combat robocalls, a broad safe harbor will also help providers respond to ever-changing robocaller tactics, when inevitably, scammers switch from one type of one-ring scam to another, or move on to other types of fraudulent schemes.

The safe harbor should also protect providers from liability due to inadvertent mislabeling or misidentification of a call's level of trust. Call labeling and call authentication solutions are important tools that are proving highly valuable in protecting consumers from robocalls. Voice service providers should be incentivized to use these innovative solutions as complements to call-blocking tools.¹⁸

While providers are committed to taking aggressive action to protect consumers, the risk of liability is still a barrier.¹⁹ Moreover, certain commenters call for the Commission to penalize voice service providers for good-faith blocking efforts,²⁰ validating earlier statements that “[t]he carriers are rightly concerned about their potential liability for blocking legitimate calls.”²¹ A broad safe harbor that shields providers from unwarranted liability for their efforts to protect consumers from all illegal and unwanted robocalls will more effectively encourage providers to maximize those efforts.

because other factors had “muddied the legal waters for voice service providers”).

¹⁸ Labeling calls with caller ID information such as “scam likely” or “fraud likely” or other formulations are a useful complement to call blocking. See *One-Ring Scams NPRM* ¶ 24 (asking whether labeling is a “useful alternative” to blocking”).

¹⁹ For example, despite the Commission’s greenlight for opt-out programs, some providers report that they favor labeling by default as opposed to blocking by default for fear of liability.

²⁰ See, e.g., Comments of Encore Capital Group, CG Docket No. 17-59, WC Docket No. 17-97, at 8–9 (Jan. 29, 2020) (calling for a white list and arguing that “there should be a penalty assessed to service providers that mistakenly block numbers on the white list.”).

²¹ Letter from Michele A. Shuster, Counsel, Professional Association for Customer Engagement, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, at 2–3 (filed May 29, 2019).

Further, in the bipartisan TRACED Act, Congress directed the Commission to establish a broad safe harbor by December 2020, and the Commission should act expeditiously in doing so. Congress confirmed the wisdom of a broad safe harbor, directing the Commission 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 [SHAKEN/STIR].”²² This language is consistent with a safe harbor for blocking based on “reasonable analytics,” which may include SHAKEN/STIR data, as well as other inputs such as spoofed phone numbers, consumer answer-rates, consumer complaints, and other data indicative of one-ring scams and other types of illegal and unwanted robocalls.

Finally, as CTIA has previously noted, the record is replete with support for a broad safe harbor.²³ Adopting a broad safe harbor would help ensure that providers have the flexibility needed to continue to use all available robocall mitigation solutions to combat one-ring scams and other illegal and unwanted traffic.

IV. CONCLUSION.

CTIA and its member companies appreciate the Commission’s dedication to protecting consumers from robocalls by encouraging providers to block one-ring scams. By also adopting a broad safe harbor that encourages providers to use all available tools, the Commission will

²² *TRACED Act*, § 4(c)(1)(B).

²³ *See, e.g.*, Letter from Michael R. Romano & Brian J. Ford, NTCA – The Rural Broadband Association, to Marlene H. Dortch, FCC, CG Docket No. 17-59, WC Docket No. 17-97 (filed Feb. 12, 2020); ; Comments of AT&T, CG Docket No. 17-59, WC Docket No. 17-97, at 6, 10 (filed July 24, 2019); Comments of T-Mobile, CG Docket No. 17-59, WC Docket No. 17-97, at 7-8 (filed Jan. 29, 2020); Comments of T-Mobile, CG Docket No. 17-59, WC Docket No. 17-97, at 8-9 (filed July 24, 2019); Comments of Verizon, CG Docket No. 17-59, WC Docket No. 17-97, at 1 (filed Jan. 29, 2020); Comments of ACA Connects, CG Docket No. 17-59, at 7 (filed July 24, 2019); Comments of First Orion Corp., CG Docket No. 17-59, WC Docket No. 17-97, at 10 (filed July 24, 2019); Comments of Transaction Network Services, CG Docket No. 17-59, at 3 (filed Sept. 24, 2018); Comments of The USTelecom Association, CG Docket No. 17-59, at 4 (filed Sept. 24, 2018); *see also* Comments of CTIA, CG Docket No. 17-59, WC Docket No. 17-97, at 7 n.22 (filed July 24, 2019).

provide consumers with even greater protection from one-ring scams and other illegal and unwanted 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

June 19, 2020