Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementing Section 503 of RAY BAUM'S Act	)	WC Docket No. 18-335
	)	
Rules and Regulation Implementing	)	WC Docket No. 11-39
The Truth in Caller ID Act of 2009	)	
	)	

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

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

April 3, 2019

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementing Section 503 of RAY BAUM'S Act	)	WC Docket No. 18-335
	)	
Rules and Regulation Implementing	)	WC Docket No. 11-39
The Truth in Caller ID Act of 2009	)	

COMMENTS OF CTIA

CTIA[1] respectfully submits these comments in response to the Federal Communications Commission's ("FCC" or "Commission") Notice of Proposed Rulemaking ("NPRM") to amend the truth in caller identification rules to further combat illegal spoofed voice calls and text messages.[2]

I. INTRODUCTION.

CTIA and its member companies share the Commission's interest in maintaining the messaging ecosystem and the voice network as trusted and reliable communications platforms. CTIA's member companies have been leading efforts to protect consumers from illegal and unwanted robotexts and robocalls.[3] With the adoption of the *Wireless Messaging Declaratory Ruling*,[4] the Commission took an important stand on behalf of wireless consumers in the battle to

[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] *Implementing Section 503 of RAY BAUM'S Act*, WC Docket No. 18-335, Notice of Proposed Rulemaking, FCC 19-12 (Feb. 14, 2019) ("*NPRM*").

[3] For the purposes of this filing, we use the terms "robocalls" and "robotexts" to refer to illegal and unconsented to robocalls and robotexts.

[4] *Petitions for Declaratory Ruling on Regulatory Status of Wireless Messaging Service*, WT Docket No. 08-7, Declaratory Ruling, FCC 18-178 (Dec. 12, 2018) ("*Wireless Messaging Declaratory Ruling*").

safeguard messaging from robotexters who want to send unwanted, malicious, and unlawful mobile messages. Further, wireless providers are undertaking an aggressive, multi-pronged approach to combat illegal robocalls.

CTIA appreciates Congressional efforts to expand the scope of the truth in caller identification rules to further combat unwanted messaging and voice traffic. The RAY BAUM'S Act directs the FCC to apply anti-spoofing requirements to text messages, and it extends the reach of rules for text messages and voice calls to include bad actors outside of the United States. In implementing the RAY BAUM'S Act, CTIA urges the Commission to use the definition of "text message" from the *Wireless Messaging Declaratory Ruling*, which would provide necessary certainty to the scope of the Commission's anti-spoofing rules. CTIA also supports the FCC aggressively enforcing its rules, within and outside of the United States, and encourages the Commission and other federal agencies to take even more steps to deter bad actors.

By adopting the proposed rules with CTIA's suggestions described herein, the Commission will help to maintain wireless text messaging services as a trusted medium for consumers that, in contrast to voice calls and email, remains virtually spam-free. Adopting the proposed rules will also enhance the Commission's ability to combat illegal robocalls that originate outside of the United States.

II. THE WIRELESS INDUSTRY SUPPORTS THE COMMISSION'S EFFORTS TO FURTHER COMBAT ILLEGAL AND UNWANTED ROBOTEXTS AND ROBOCALLS IN THIS PROCEEDING.

A. As the *Wireless Messaging Declaratory Ruling* Affirmed, Wireless Providers Are on the Frontlines in Protecting Consumers from Illegal and Unwanted Text Messages in Order to Maintain the Messaging Ecosystem as a Trusted Communications Medium.

Text messaging is a dynamic and evolving service that consumers trust. As the Commission recognized in the *Wireless Messaging Service Declaratory Ruling*,

> [t]exting has evolved into one of the most popular forms of communication for Americans, with trillions of wireless text messages sent each year in the United States. The tremendous growth of wireless messaging is attributable in large part to the fact that providers have been able to ensure the relatively spam-free nature of this service, which in turn has spurred a high degree of consumer loyalty to this method of communication, especially among younger Americans.[5]

This ecosystem is an attractive target for bad actors: "Unfortunately, always-on communications, inherent trust in the channel, high open rates, and six billion subscribers are not lost on those with ill intent. Just as SMS provides a successful avenue for legitimate businesses to correspond with its customers, those hoping for illicit profits are also trying to cash in."[6] However, wireless messaging remains trusted because wireless providers take a variety of steps to mitigate significant quantities of unwanted message traffic from reaching consumers.

The trusted messaging ecosystem stands in stark contrast to the undeniable problem of illegal robocalls and spam in the emailing ecosystem. The spam rate via SMS is estimated at 2.8 percent,[7] compared to an estimated e-mail spam rate of over 50 percent.[8] Surveys confirm that consumers recognize text messaging as the most dependable means of avoiding unwanted communications. In a recent Morning Consult survey, nearly 90 percent of consumers identified voice and email traffic – not text messages – as the platform where they receive the most unwanted communications.[9] Not surprisingly, 91 percent of surveyed consumers support

---

[5] *Wireless Messaging Declaratory Ruling* ¶ 1 (citations omitted).
[6] Cloudmark, *SMS Spam Overview: Preserving the value of SMS texting*, at 2, https://www.cloudmark.com/releases/docs/whitepapers/SMS_Spam_Overview.pdf (last visited Mar. 28, 2019) ("*Cloudmark SMS Spam Overview*").
[7] *See* Letter from Matthew Gerst, Assistant Vice President, Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, WT Docket No. 18-28, at 3 (filed Nov. 16, 2018) ("*Nov. 2018 CTIA Ex Parte Letter*"); *see also Wireless Messaging Declaratory Ruling* ¶ 12.
[8] *See* Maria Vergelis, Tatyana Shcherbakova & Tatyana Sidorina, *Spam and phishing in 2018* (Mar. 12, 2019), https://securelist.com/spam-and-phishing-in-2018/89701/ (global average email spam rate in 2018 was 52.48 percent); Symantec, *2019 Internet Security Threat Report, Volume 24*, at 23, 29 (Feb. 2019), *available at* https://www.symantec.com/security-center/threat-report (spam accounted for 55 percent of email globally in 2018); *see also* Kim Fai Kok, *2018 U.S. Spam & Scam Report*, Truecaller (Apr. 26, 2018), https://blog.truecaller.com/2018/04/26/truecaller-insights-usa-2018/.
[9] *See Dec. 2018 CTIA Ex Parte Letter* at 1-2.

wireless providers' efforts to identify and block spam, according to a November 2018 survey.[10]

The messaging ecosystem remains "safe and trusted"[11]—or "least polluted"—because messaging providers, including wireless providers, actively manage the platforms to protect consumers against illegal robotexts. Among other tools, providers employ spam filtering software and account fingerprinting to identify suspicious accounts. CTIA has developed *Messaging Principles and Best Practices* that help to protect consumers from unwanted texts and support a robust and dynamic wireless messaging ecosystem where wanted messages can be exchanged between and among enterprises and consumers, and consumers are protected from unwanted messages, including in conformity with applicable laws and regulations, such as the Telephone Consumer Protection Act.[12]

As an additional example, AT&T reports that, among other things, it is helping "identify trusted traffic and minimize inadvertent blocking" by

- Using a "'tagging' pilot which assigns a trust level to traffic from trusted senders subjecting it to more limited spam filters, reducing the potential for inadvertent blocking and time to rectify any blocking issues"
- "[A]dopting [a] Code of Conduct with simple rules and recommendations for aggregator partners" to help legitimate traffic flow freely and targeting scammers' practices and
- Developing "Feedback Loops to proactively inform aggregators of operational spam issues as they are discovered."[13]

Other carriers are exploring solutions as well. Thus, the Commission was right to affirm

---

[10] *See* Letter from Matthew Gerst, Assistant Vice President, Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, WT Docket No. 08-7, at 1-2 (filed Dec. 6, 2018) ("*Dec. 2018 CTIA Ex Parte Letter*").

[11] *Cloudmark SMS Spam Overview* at 2.

[12] *See* CTIA, *Messaging Principles and Best Practices* (Jan. 19, 2017), https://api.ctia.org/docs/default-source/default-document-library/170119-ctia-messaging-principles-and-best-practices.pdf; *Nov. 2018 CTIA Ex Parte Letter; see also*, Messaging, Malware and Mobile Anti-Abuse Working Group, *M3AAWG Mobile Messaging Best Practices for Service Providers*, at 3 (updated Aug. 2015), https://www.m3aawg.org/sites/default/files/M3AAWG-Mobile-Messaging-Best-Practices-Service-Providers-2015-08.pdf (which "defines a set of voluntary best practices for service providers and vendors to assist in the creation and maintenance of the highest practical levels of trust and security attainable in an open, globally-interconnected messaging environment.".

[13] *See* Letter from Celia Nogales, Assistant Vice President, Regulatory, AT&T, to Marlene H. Dortch, Secretary, FCC, WT Docket No. 08-7, at 1-2 (filed Dec. 6, 2018).

that wireless messaging is an information service in the *Wireless Messaging Declaratory Ruling* in order to maintain wireless providers' ability to protect consumers from illegal and unwanted messages through these and other robust measures.

B. The RAY BAUM'S Act Complements Wireless Providers' Aggressive, Multi-Pronged Approach to Illegal Robocalls.

In furtherance of the Commission's efforts to mitigate illegal robocalls, the extension of anti-spoofing rules to reach bad actors outside of the United States under the RAY BAUM'S Act will empower the Commission with new authority and capabilities to work with the wireless industry to relieve consumers from the plague of illegal robocalls.

While there is no silver bullet solution that will stop illegal robocalls, voice service providers, including wireless carriers, the Commission, law enforcement, and other ecosystem stakeholders have been working together to develop and deploy a variety of tools to protect consumers and the voice network.[14] One example of an anti-spoofing innovation that providers are in the process of implementing is SHAKEN/STIR, which is a set of IP-based standards that are designed to authenticate calls and mitigate spoofing.[15] SHAKEN—which stands for "Signature-based Handling of Asserted information using toKENs"—and STIR—which stands for "Secure Telephone Identity Revisited"—were industry developed through a consensus process led by ATIS and the SIP Forum. SHAKEN/STIR is a set of leading-edge cryptographic protocols and operational procedures to authenticate calls and mitigate spoofing and associated illegal robocalling.

Implementing SHAKEN/STIR will help give consumers more choice and control over

[14] *See, e.g.*, *Robocall Strike Force Report*, at 3 (Oct. 26, 2016), https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf ("*2016 Robocall Strike Force Report*").
[15] *See* Carrier Responses to Letter from Chairman Ajit Pai Regarding Call Authentication (Nov. 2018), https://www.fcc.gov/call-authentication.

how to avoid unauthenticated calls, including by blocking such calls. Stakeholders are working to develop consumer-facing displays associated with SHAKEN/STIR, and the wireless industry is committed to ensuring that consumers reap its benefits as soon as possible.

Further, wireless providers aggressively use a variety of tools to prevent illegal robocalls. For example, wireless providers are working to stop illegal robocalls before they reach consumers. Wireless providers have embraced carrier-initiated blocking of calls originated from unassigned telephone numbers consistent with the Commission's rules.[16] Additionally, CTIA and its member companies have expressed support for the adoption of the bipartisan TRACED Act.[17] The TRACED Act, as recently reintroduced, is intended to strengthen the Commission's enforcement tools, encourage adoption of SHAKEN/STIR, and provide safe harbors for carriers that use call authentication. If adopted, the TRACED Act's safe harbors would help the Commission provide more certainty for providers to take aggressive actions against unauthenticated robocalls.

Complementing this work, providers are collaborating with the Commission and law enforcement to identify and root out bad actors through USTelecom's traceback efforts,[18] which coordinate industry efforts to identify the source of illegal robocalls. Many of CTIA's member companies are longstanding members of USTelecom's Industry Traceback Group ("ITB Group").[19] In addition to wireless providers, the ITB Group's 20+ members include traditional

---

[16] *See, e.g.*, Letter from Joan Marsh, Chief Regulatory & State External Affairs Officer, AT&T, to Commissioner Jessica Rosenworcel, CG Docket No. 17-59 (filed Jan 14, 2019), https://docs.fcc.gov/public/attachments/DOC-355921A2.pdf; Comments of CTIA, CG Docket No. 17-59 (Sept. 24, 2018).

[17] *See*, S.151, Telephone Robocall Abuse Criminal Enforcement and Deterrence Act ("TRACED Act"), 116th Congress (to deter criminal robocalls violations and improve enforcement of section 227(b) of the Communications Act of 1934, and other purposes).

[18] *See* FCC Letter to USTelecom Regarding Industry Traceback Group (Nov. 6, 2018), https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf.

[19] *See, e.g.*, Comments of the USTelecom Association, CG Docket No. 17-59, pp. 6 – 9 (September 24, 2018).

wireline phone companies, transit providers, and cable companies. Since late 2017, it has been investigating the source of illegal robocalls and making enforcement referrals to the FCC and the Federal Trade Commission. While all of these efforts unfold, providers and other ecosystem stakeholders, including the application developers, are offering a wide variety of tools to empower consumers, like labeling and blocking tools.[20]

In sum, wireless providers and voice service stakeholders are employing innovative and aggressive tools to stop illegal robocalls at every stage in call transmission. CTIA and its member companies stand ready to continue working with the Commission to relieve consumers from the plague of illegal robocalls.

III. AS IT EXPANDS ANTI-SPOOFING RULES TO MESSAGING, THE COMMISSION SHOULD ENSURE THAT THE DEFINITION OF "TEXT MESSAGE" IN THE ANTI-SPOOFING RULES IS CONSISTENT WITH THE *WIRELESS MESSAGING DECLARATORY RULING.*

CTIA supports expanding the anti-spoofing rules to implement the RAY BAUM'S Act in a manner consistent with the *Wireless Messaging Declaratory Ruling.* Specifically, for purposes of clarity and consistency, the Commission should define the scope of the expanded anti-spoofing rules to include Short Message Service (SMS) and Multimedia Message Service (MMS) text messages as those terms were defined in the *Wireless Messaging Declaratory Ruling*.

There, the Commission defined SMS as a "wireless messaging service" that "enables users to send and receive short text messages, typically 160 characters or fewer, to or from mobile phones and can support a host of applications."[21] Further, the Commission affirmed that

[20] *See* Carrier Responses to Letter from Commissioner Jessica Rosenworcel Regarding Call Authentication (Jan. 2019), https://docs.fcc.gov/public/attachments/DOC-355921A2.pdf.
[21] *Wireless Messaging Declaratory Ruling* ¶ 8.

MMS is "an extension of the SMS protocol and can deliver a variety of media, and enables users to send pictures, videos, and attachments over wireless messaging channels."[22]

For purposes of expanding the scope of the Commission's anti-spoofing rules to text messages, the RAY BAUM'S Act defined a "text messaging service" as a service that routes messages to 10-digit telephone numbers or N11 service codes (telephone numbers) that might be spoofed.[23] In order to ensure clarity and certainty as to the scope of covered services, the Commission should interpret "text messaging service" for anti-spoofing rules to include SMS and MMS.

IV. CTIA SUPPORTS THE COMMISSION'S EFFORTS TO STEP UP ENFORCEMENT OF ANTI-SPOOFING RULES AGAINST BAD ACTORS, INCLUDING BY EXPANDING THE REACH OF THE RULES TO THOSE WHO OPERATE OUTSIDE OF THE UNITED STATES.

The Commission should continue to prioritize enforcement against bad actors who exploit the trust that was inherent among voice services to flood consumers with illegal robocalls. In so doing, the Commission should ensure its anti-spoofing rules apply broadly throughout the voice system and work with peer agencies to increase effectiveness of enforcement against bad actors. Consistent with the RAY BAUM'S Act, CTIA supports the Commission's proposed rule that

> No person or entity in the United States, *nor any person or entity outside the United States if the recipient is within the United States*, shall, with the intent to defraud, cause harm, or wrongfully obtain anything of value, knowingly cause, directly, or indirectly, any caller identification service to transmit or display misleading or inaccurate caller identification information in connection with any voice service or text messaging service.[24]

---

[22] *Id.*
[23] *See* Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 1084, Division P–RAY BAUM'S Act of 2018, § 503(a)(2)(C)-(D) (defining both "text message" and "text messaging service") ("*RAY BAUM'S Act*").
[24] *NPRM* at 15 (emphasis added); *see RAY BAUM'S Act*, §503(a)(1).

As Commission staff recently noted in the *Report on Robocalls*, a major challenge in illegal robocall enforcement is that "many illegal robocallers are operating in foreign countries."[25] Thus, expanding the reach of the rules to these bad actors is a necessary and important step in the continued fight against illegal robocalls.

In conjunction with the aggressive and on-going work to stop illegal robocalls and robotexts by the Commission and industry, the Commission should redouble its enforcement efforts against bad actors. While CTIA commends the FCC's recent enforcement actions against perpetrators of illegal robocalls,[26] we urge the Commission to continue to pursue aggressive enforcement against illegal robocallers that seek to defraud consumers by concealing their identity through spoofed telephone numbers. The entire ecosystem, from consumers to legitimate calling parties, will benefit from aggressive pursuit of those who flout the Commission's truth in caller identification rules.

Further, CTIA and its member companies support additional steps by the Commission to intensify efforts against bad actors. Foremost, the Commission should aggressively exercise the expanded authority to enforce its rules against bad actors outside of the U.S. that Congress provided with the RAY BAUM'S Act. Additionally, the Commission should work with federal partners to ensure that the historic fines levied by the Commission against illegal robocallers are paid, thereby creating a significant deterrent to bad actors for breaking the law.[27] Overall, the

---

[25] *Report on Robocalls*, CG Docket No. 17-59, ¶ 38 (Feb. 2019), https://docs.fcc.gov/public/attachments/DOC-356196A1.pdf.

[26] *See, e.g.*, *Best Insurance Contracts, Inc., and Philip Roesel, dba Wilmington Insurance Quotes*, Forfeiture Order, FCC 18-134 (Sept. 26, 2018) ($82 million for illegally-spoofed robocalls); *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, Forfeiture Order, FCC 18-58 (May 10, 2018) ($120 million for neighbor spoofing robocall operation).

[27] S. Krause, *The FCC Has Fined Robocallers $208 Million. It's Collected $6,790*, Wall St. J. (Mar. 28, 2019) https://www.wsj.com/articles/the-fcc-has-fined-robocallers-208-million-its-collected-6-790-11553770803 (noting that bad actors continue to break the law and avoid punishment despite the Commission's aggressive enforcement and large forfeiture orders).

Commission should work with relevant government agencies, including the Federal Trade Commission and the U.S. Department of Justice, as well as states attorneys general and international counterparts, through a "whole of government" approach to ensure both foreign and domestic bad actors are sufficiently deterred and consumers are relieved from the scourge of illegal robocalls.[28]

V. CONCLUSION.

CTIA appreciates and supports the Commission's continued efforts to relieve consumers from the scourge of illegal robocalls and maintain wireless text messaging services a trusted medium for consumers. By adopting the proposed rules consistent with CTIA's comments, the Commission will provide necessary certainty and clarity to the scope of the anti-spoofing rules over text message services, as well as enhance the Commission's ability to combat illegal robocalls originated outside of the U.S.

[28] *See Report on Robocalls* ¶ 38.

Respectfully submitted,

/s/ Matthew Gerst

Matthew Gerst
Vice President, Regulatory Affairs

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

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

April 3, 2019