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

In the Matter of	)	
	)	
Targeting and Eliminating Unlawful Text Messages	)	CG Docket No. 21-402
	)	

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Sarah Leggin
Director, Regulatory Affairs

CTIA
1400 Sixteenth Street, N.W.
Suite 600
Washington, D.C. 20036
(202) 736-3220

November 10, 2022

TABLE OF CONTENTS

I. INTRODUCTION & SUMMARY....1

II. TEXT MESSAGING IS A POPULAR AND TRUSTED MEDIUM BECAUSE OF THE WIRELESS INDUSTRY'S ACTIVE MANAGEMENT AND ITS EVOVLVING EFFORTS TO PROTECT CONSUMERS. 6

III. THE COMMISSION'S ROBOCALL BLOCKING REGIME AND CALLER ID AUTHENTICATION MANDATE WERE PURPOSE-BUILT FOR VOICE CALLS AND ARE NOT APPLICABLE TO TEXT MESSAGING. 10

A. The Problems that the Robocall Rules Address are Not the Problems that Enable Spam Text Messages....10

B. The Solutions the Commission Adopted to Address Robocall Problems Do Not Address the Problems that Enable Spam Text Messages. 12

1. The Commission's Blocking Proposal in the *Notice* Could Undermine the Anti-Spam Framework for Messaging That Protects Consumers Today. 12

2. The Caller ID Authentication Proposal Imported From the Robocall Playbook Does Not Apply to the Messaging Technology or Issues That Industry Is Already Addressing. 17

IV. THE COMMISSION CAN BEST PROTECT CONSUMERS FROM UNWANTED AND ILLEGAL TEXT MESSAGES BY ENHANCING INFORMATION-SHARING CAPABILITIES, ENFORCING EXISTING RULES, AND SUPPORTING INDUSTRY EFFORTS. 19

V. CONCLUSION. 22

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

In the Matter of	)	
	)	
Targeting and Eliminating Unlawful Text Messages	)	CG Docket No. 21-402
	)	

COMMENTS OF CTIA

CTIA[1] respectfully submits these comments in response to the Federal Communications Commission's ("Commission" or "FCC") Notice of Proposed Rulemaking ("*Notice*") seeking comment on how best to protect consumers from illegal and unwanted text messages.[2]

I. INTRODUCTION & SUMMARY.

Wireless text messaging is one of Americans' most popular forms of communication,[3] used to communicate with friends and family, emergency responders, and innovative businesses, as well as for just-in-time notifications regarding health care, education, employment, travel, finance, civic participation and more. That success exists because of consumers' trust in the

[1] CTIA —The Wireless Association® ("CTIA") (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Targeting and Eliminating Unlawful Text Messages*, Notice of Proposed Rulemaking, FCC 22-72 (rel. Sept. 27, 2022) ("*Notice*").

[3] *Id.* ¶ 1; FCC, Consumer Advisory Committee, *Report on the State of Text Messaging*, at 5 (Aug. 30, 2022) ("CAC Report"), https://files.fcc.gov/ecfs/download/20970528-9c2e-400d-951b-1024118e50fb?orig=true&pk=cb77b2ec-1a58-dbc6-139b-ad192cfd5d9b.

messaging platform—and that trust is why messaging has a 98% open rate.[4] The wireless industry wants to keep it that way, and that is why CTIA and our member companies are committed to maintaining consumer trust and confidence in wireless text messaging.

As the Commission's Consumer Advisory Committee ("CAC") recently observed, the wireless industry has taken measures to promote innovative uses of the text messaging platform while also combatting unwanted messages, even as messaging's popularity has made it a more attractive target for bad actors.[5] Between 2015 and 2020, while the total volume of text messages increased from over 1 trillion to over 2 trillion, the number of spam text messages that wireless providers blocked grew ten times, from an estimated 1.4 billion in 2015 to 14 billion in 2020.[6] The wireless industry continues to evolve the playbook to keep protecting consumers from spam messaging even as bad actors change their tactics—successfully preventing billions of spam text messages from ever reaching consumers each year. And, blocking is only part of the broader effort to protect consumers from spam text messages.

Messaging stakeholders vigorously employ and are enhancing up-front vetting and monitoring solutions, sophisticated filtering algorithms, and fraud investigations as well as developing and promoting messaging principles and security best practices to protect consumers and the platform. In fact, these efforts are protecting messaging far better than other platforms, such as email for example.[7] And, the wireless industry is committed to improving the consumer

---

[4] CAC Report at 5.

[5] *Id.* at 6-7; *See also, e.g.*, *Notice* ¶ 3 (describing the increase in complaints about spam texts in the past 12-18 months).

[6] CTIA, *Annual Survey Highlights* (Sept. 13, 2022), https://www.ctia.org/news/2022-annual-survey-highlights.

[7] Last year, consumers submitted just one complaint for every 68.4 million SMS/MMS messages sent. *Comparing* FCC, Consumer Compliant Data Center, https://www.fcc.gov/consumer-help-

experience by launching new tools and resources, including CTIA's new *Fighting Spam* feature page that explains how the wireless industry protects consumers, what consumers should expect from senders, and ways to avoid and report spam texts.[8] The wireless industry is also increasing coordination among industry, policymakers, and law enforcement through CTIA's new *Secure Messaging Initiative* and other efforts to crack down on the bad actors that are behind spam texts.[9]

But bad actors are not only targeting SMS/MMS texting—they are increasingly seeking to use a variety of platforms, including over-the-top ("OTT") applications like WhatsApp, social media platforms like Facebook, and more to harm consumers. All messaging stakeholders—including OTT providers, cloud platforms, aggregators, and others—have a role to play in the effort to prevent spam messages and deter bad actors from targeting consumers.[10] Indeed, just a few years ago, OTT messaging comprised nearly 75% of all messaging traffic. Today, that number is closer to 85%.[11] As CTIA's *Messaging Security Best Practices* observe, stakeholders

---

center-data (last visited Nov. 9, 2022) *and* CTIA Annual Survey Highlights, *supra* note 6. *See also Global spam volume as a percentage of total e-mail traffic from January 2014 to December 2021, by month*, Statista (May 2022), https://www.statista.com/statistics/420391/spam-email-traffic-share/ (reporting a nearly 50% spam rate for email globally).

[8] *See* CTIA, Protecting You From Spam Text Messages, https://fightingspam.ctia.org/ (last visited Nov. 9, 2022).

[9] *See* CTIA, CTIA Secure Messaging Initiative, https://www.ctia.org/ctia-secure-messaging-initiative (last visited Nov. 9, 2022).

[10] Like wireless providers, OTT messaging providers are working actively to combat unwanted messages. *See, e.g.*, WhatsApp, About spam and unwanted messages, https://faq.whatsapp.com/1419898338168991/?locale=en_US (last visited Nov. 9, 2022); Facebook Messenger, Blocking, reporting and deleting, https://www.facebook.com/help/messenger-app/1145318292241859?helpref=search&query=spam&search_session_id=9c1f29d1aa1f96189836796c8d057031&sr=2 (last visited Nov. 9, 2022).

[11] Pamela Clark-Dickson & Charlotte Palfrey, *OTT Messaging Forecast Report: 2019-24*, Omdia (Jan. 7, 2021); CTIA Annual Survey Highlights, *supra* note 6.

throughout the ecosystem can play a significant role in helping to protect consumers from spam and support continued security and trust in the messaging ecosystem.[12] The Commission should encourage all messaging providers to continuously innovate to prevent spam messages and deter bad actors from targeting the messaging ecosystem. A regulatory approach focused on a small part of the landscape will not discourage bad actors.

CTIA shares the Commission's goal of protecting consumers from spam text messages, but the proposals in the *Notice* presuppose that transposing the Commission's robocall rules onto the messaging ecosystem will help to further reduce spam text messages.[13] As discussed in more detail below, the technology, challenges, and bad actor tactics in the messaging ecosystem are different from those that have plagued voice services. In fact, the wireless industry already is actively blocking unwanted and illegal text messages based on much more sophisticated criteria than the criteria proposed in the *Notice.* And, the *Notice* inappropriately focuses on STIR/SHAKEN as a solution for wireless text messaging. The STIR/SHAKEN caller ID authentication framework was purpose-built for session initiation protocol ("SIP") based voice services and thus cannot be layered onto messaging platforms that are supported by protocols other than SIP. Nor is there a need to do so: wireless text messaging already incorporates significant elements of authentication through registration and up-front vetting and validation. Further, the wireless industry's on-going efforts to evaluate future authentication technologies

[12] CTIA, *Messaging Security Best Practices* (June 2022) ("CTIA Messaging Security Best Practices"), https://api.ctia.org/wp-content/uploads/2022/06/Messaging-Security-Best-Practices-June-2022.pdf (providing general messaging security best practices that stakeholders may employ to help protect consumers from spam and address security concerns).

[13] *Notice* ¶ 18 ("We propose to protect consumers from the increasing numbers [sic] of illegal text messages by extending some of our consumer protections against illegal phone calls to text messages.").

and solutions are likely to yield even more actionable information to further minimize the volume of spam text messages.

Rather than adopting mandates that are ill-suited to further reduce spam text messages, the Commission should use this proceeding to advance the messaging ecosystem's efforts to combat text messaging spam, which are specifically targeted at the unique and evolving sources of spam texts. Specifically, CTIA encourages the Commission to harness the tools it has readily available to collaborate with the wireless industry to target and mitigate the harms posed by bad actors. For example, the Commission can better target bad actors through CTIA's *Secure Messaging Initiative*, which includes a clearinghouse to facilitate information-sharing among industry and government representatives. In addition, the Commission can stand up the information sharing portal mandated under the TRACED Act to enhance its coordination on enforcement efforts with industry.[14] The Commission can also enforce the Telephone Consumer Protection Act ("TCPA") and Truth in Caller ID rules, and work with the Federal Trade Commission ("FTC") and law enforcement to target bad actors. Finally, the Commission should follow through on the CAC's recommendations to encourage broader adoption of industry principles and security best practices[15] and to join the wireless industry's efforts to enhance

[14] *See Implementing Section 10(a) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, Report and Order, 36 FCC Rcd 10675 (2021) ("*TRACED Act Portal Order*").

[15] *See* CTIA, Messaging, https://www.ctia.org/homepage/messaging-channel (last visited Nov. 9, 2022) (describing how the wireless industry protects consumers from unwanted messages and providing resources for consumers and non-consumer message senders).

consumer education on the fight against spam messaging,[16] and how to avoid and report spam text messages.[17]

To maintain and expand text messaging's role as a trusted communications platform, the wireless industry will continue to innovate and keep pace with the incessantly changing tactics of bad actors. Instead of pursuing the proposals in the *Notice* that would not be effective at further reducing spam text messages, the Commission should support and collaborate with CTIA and its member companies on efforts targeted to the specific causes of text spam in order to best achieve the shared goal of protecting consumers from illegal and unwanted text messages.

II. TEXT MESSAGING IS A POPULAR AND TRUSTED MEDIUM BECAUSE OF THE WIRELESS INDUSTRY'S ACTIVE MANAGEMENT AND ITS EVOVLVING EFFORTS TO PROTECT CONSUMERS.

Wireless providers and their partners throughout the wireless messaging industry have been on the front lines of protecting consumers from illegal and unwanted text messages for years. While the industry is successfully preventing billions of spam text messages from reaching consumers each year, there is more work to be done. CTIA's member companies and their partners throughout the wireless messaging ecosystem are constantly developing new tools to thwart bad actors' ever-changing and increasingly complex tactics.

Since its launch in 1992, text messaging has evolved into one of the most popular forms of communication for Americans, with trillions of wireless text messages sent each year in the U.S. In 2021, American consumers exchanged 2 *trillion* text messages—over 63,600 text

[16] CTIA Protecting You From Spam Text Messages, *supra* note 8 (describing how the wireless industry protects consumers from unwanted messages).

[17] *See* CTIA, Protecting Yourself From Spam Text Messages, https://www.ctia.org/consumer-resources/protecting-yourself-from-spam-text-messages (last visited Nov. 9, 2022) (describing ways for consumers to report and manage spam text messages).

messages per second.[18] SMS open rates are estimated to be 98 percent,[19] and response rates are as high as 45 percent.[20] This is much higher than email, with a 20 percent open rate and 6 percent response rate.[21] The uniquely trustworthy nature of text messaging is a direct result of conscious and extensive actions by wireless providers and other stakeholders in the messaging ecosystem.

As a threshold protection against unwanted and illegal text messages, wireless providers require up-front vetting for entities that seek to originate bulk text messages. By requiring non-consumers to submit to up-front vetting with entities that facilitate the flow of messaging traffic among each mobile wireless network, including aggregators and registrars, this process deters bad actors from seeking access to messaging platforms in the first instance. It also enhances transparency to help ensure legitimate messages go through and to help identify messages from un-registered, un-vetted sources.[22]

Further, the architecture of wireless messaging networks is such that wireless providers know the transmitting provider (e.g., wireless provider or messaging solutions aggregator) and user identifier (whether telephone number/long code, short code, or other marker) for text messages. With this information, wireless providers typically deliver text messages only from authorized providers and user identifiers using valid originating information through appropriate routing channels. And this information helps providers identify bad actors by enhancing the ability to detect and stop suspicious messages that are not flowing through appropriate channels.

---

[18] CTIA Annual Survey Highlights, *supra* note 6.

[19] *Id.*; *see also* CAC Report at 5.

[20] CAC Report at 5.

[21] *Id.*

[22] *See id.* at 8-9, 16-17.

To maintain consumer trust and promote growth of the messaging platform, the wireless industry has established guidelines to encourage the innovative use of messaging by a variety of stakeholders, while also guarding against unwanted and unlawful text messages. For example, CTIA's *Messaging Principles and Best Practices* establish expectations that non-consumer message senders will obtain consumer consent prior to messaging consumers, and that they will honor consumer opt-outs, among other practices.[23] These guidelines are mutually applied by messaging ecosystem stakeholders through commercial agreements and policies to protect consumers from unwanted messages and maintain consumer trust.[24]

In addition to these frontline processes and best practices, messaging stakeholders use a variety of trained experts and automated tools to protect consumers and combat spam text messages while also protecting legitimate messages. Wireless providers' security and fraud prevention teams use innovative technologies, machine learning, and other spam mitigation tools to protect consumers through real-time analysis and other defense solutions. For example, when wireless providers receive complaints about texts with suspicious URLs or domains, they investigate the website to determine if the link is intended to support fraudulent efforts. If so, wireless providers can share the fraudulent link with Google's Safe Search list,[25] so it can be blocked by most internet browsers and limit the potential for consumers to interact with the scam.

To enhance these protections, wireless providers have established a common means for consumers to report unwanted text messages—7726 (SPAM). Wireless providers track and

---

[23] CTIA Messaging Security Best Practices at 6.

[24] CAC Report at 6 & n.10 (citing wireless provider policies).

[25] Google Search Help, Filter explicit results using SafeSearch, https://support.google.com/websearch/answer/510?hl=en&co=GENIE.Platform%3DAndroid (last visited Nov. 9, 2022).

aggregate the information that consumers report to them through 7726 and, together with industry partners, use that data to further calibrate their spam filters and blocking tools. New reporting tools have also been deployed onto messaging applications that are native to wireless device operating systems and provide consumers with a more streamlined means of reporting spam text messages.[26] Wireless providers use these reports and other detailed data about text messages to modify rules-based protocols—constantly evolving spam mitigation tools in real-time to keep pace with the incessantly changing tactics of bad actors described below.

The wireless industry's management of messaging services gives providers and other stakeholders many tools and information sources to identify and mitigate unwanted messages. Industry shares this information with the Commission, the FTC, state attorneys general, and law enforcement in an effort to collaboratively stop bad actors. To advance these efforts, CTIA launched the *Secure Messaging Initiative* to further the wireless industry's efforts to stop unwanted or illegal text messaging.[27] The initiative includes a central clearinghouse that providers and government agencies can use to share information about and take action on suspected spam messages and techniques, as well as new *Messaging Security Best Practices* to provide guidance to stakeholders on how to address leading sources of unwanted messaging.[28]

In sum, wireless providers and their messaging ecosystem partners are focused on maximizing consumers' trust in the messaging platform by mitigating unwanted and illegal text

[26] *See, e.g.*, Apple, Block, filter, and report messages on iPhone, https://support.apple.com/-guide/iphone/block-filter-and-report-messages-iph203ab0be4/ios (last visited Nov. 9, 2022); Google Android, Report Spam, https://support.google.com/messages/answer/9061432?hl=en (last visited Nov. 9, 2022).

[27] *See* CTIA Secure Messaging Initiative, *supra* note 9.

[28] *Id.*

messages, and are constantly evolving their capabilities to protect consumers and keep up with bad actors.

III. THE COMMISSION'S ROBOCALL BLOCKING REGIME AND CALLER ID AUTHENTICATION MANDATE WERE PURPOSE-BUILT FOR VOICE CALLS AND ARE NOT APPLICABLE TO TEXT MESSAGING.

CTIA and its member companies share the Commission's goals and are committed to continued investment in innovative solutions necessary to combat the ever-evolving threat landscape—across all platforms. For years, the wireless industry has supported the Commission's efforts to protect consumers from robocalls. However, the *Notice*'s proposal to extend regulation adopted against illegal phone calls to text messages will not protect consumers from spam text messages because different challenges and technologies require different solutions.[29]

A. The Problems that the Robocall Rules Address are Not the Problems that Enable Spam Text Messages.

The Commission's robocall blocking regime and authentication obligations were designed to address issues specific to voice calls—in particular, unwanted and illegal calls being transmitted with no caller ID information or falsified caller ID information and no identification of the originating carrier. These issues were exacerbated by a lack of clarity about the scope of common carrier voice providers' ability to block calls.[30]

[29] *Notice* ¶ 18.

[30] *See, e.g., Advanced Methods to Target and Eliminate Unlawful Robocalls,* Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706, 9726 ¶ 60 (2017) ("*2017 Call Blocking Order*") (clarifying that call blocking consistent with the requirements adopted therein was permissible despite the requirements of 47 U.S.C. §§ 201-202); *see also id.* at 9709 ¶ 9 & n.28 (citing rural call completion rules at 47 C.F.R. § 64.2101 *et seq.*).

The challenges presented by spam text messages, however, are different. First, spam messages are not generally delivered using invalid, unallocated, unused, or do-not-originate ("DNO") telephone numbers. In fact, on mobile messaging networks, generally only valid, authorized telephone numbers can be used to send text messages.[31] Robust, existing countermeasures prevent messages from invalid, unallocated, unused or DNO telephone numbers from being transmitted to consumer's wireless devices.

As a result, bad actors employ a variety of other techniques to transmit spam text messages from valid telephone numbers. As the CAC found, some bad actors exploit low barriers to *legitimately* access telephone numbers through low-cost prepaid Subscriber Identification Module ("SIM") cards or electronic SIM cards.[32] Others use social engineering tactics to take over *legitimate* message sender accounts.[33] As the CAC recounts, wireless providers are confronting these issues through rigorous and evolving spam filtering and blocking solutions, as well as up-front vetting, registry requirements, and monitoring of traffic sent by

[31] Comments of WMC Global, CG Docket No. 21-402, at 2 (filed Oct. 21, 2022) ("Brand Impersonation is sometimes referred to as spoofing or brand spoofing, but it is not the same as text message spoofing, which indicates technical sophistication. Text message spoofing, or number spoofing, does not specifically have to be brand related and, in our experience, is extremely uncommon in the US because the technology to accomplish this spoofing is not the same as in other international markets.").

[32] CAC Report at 11; *see also*, Press Release, Transaction Network Services, *TNS Robocall Report: Robocalls Down 8% in 2022, accelerated by STIR/SHAKEN and Regulatory Enforcement* (Oct. 31, 2022) ("TNS Press Release"), https://tnsi.com/resource/tns-robocall-report-robocalls-down-8-in-2022-accelerated-by-stir-shaken-and-regulatory-enforcement/ (noting that "spammers and scammers seize on disposable, text-enabled ten-digit telephone numbers that can be easily obtained through web-based services or pre-paid SIM cards. Nearly half of robotext scams during the first half of 2022 originated from bad actors using snowshoe messaging techniques, where the sender spreads their attack across multiple telephone numbers.").

[33] CAC Report at 11.

non-consumer message senders.[34] But these issues—which are at the root of spam text messages—are different from the issues that underlie robocalls.

B. The Solutions the Commission Adopted to Address Robocall Problems Do Not Address the Problems that Enable Spam Text Messages.

Because the problems underlying text messages are different from the problems underlying robocalls, application of robocall solutions will not effectively protect consumers against text spam. The Commission's rules clarifying voice service providers' authority to block calls and adopting a specific call authentication framework, STIR/SHAKEN, are helping industry respond to the problems that robocalls presented.[35] Wireless providers were strong supporters of those Commission actions, encouraging adoption of rules to provide clarity on call blocking and moving more rapidly than other voice providers to deploy STIR/SHAKEN. These solutions, however, will not protect consumers from unwanted and illegal and unwanted text messages.

1. The Commission's Blocking Proposal in the *Notice* Could Undermine the Anti-Spam Framework for Messaging That Protects Consumers Today.

As part of its efforts to reduce the volume of robocalls reaching consumers, the Commission clarified that voice service providers are permitted to block certain calls. However, the rationale and regulatory framework that supported those rules in the robocall context do not support the text message blocking mandate proposed in the *Notice*.

---

[34] *Id.* at 16-17.

[35] TNS Press Release ("Progress by top US carriers implementing STIR/SHAKEN, aggressive regulatory enforcement efforts, and the use of advanced call analytics helped drive down robocall volume 8% in the first half of 2022 compared to the same period last year (from 37.9 billion down to 34.9 billion).").

As noted above, text spammers do not generally rely on invalid, unallocated or unused numbers, or numbers on the DNO List, and so the proposed blocking mandate would offer little relief to consumers. At the same time, wireless text messaging providers already are empowered to protect consumers from unwanted and illegal text messages,[36] and they work aggressively and creatively to do so.[37] As the CAC Report observed, "[c]ompared to the robocall context, where there is different data available to identify illegal and unwanted calls, innovative technologies in the messaging ecosystem apply sophisticated algorithms, which may include machine learning and artificial intelligence elements, to detailed data about text messages to enhance existing spam mitigation tools."[38] These tools enable wireless providers to block text messages based on volume, consumer complaints, and other evidence of fraud or malfeasance, including compromised API credentials, utilization of grey routes, lack of authentication, or a pattern of abuse of industry best practices—a far more comprehensive approach that the Commission proposes in the *Notice*.[39]

The blocking rule proposed in the *Notice* will do little in the way of offering protection for consumers who are already benefitting from the robust anti-spam blocking regime that wireless providers have today. In fact, the proposed blocking rule, while narrower in scope than current industry efforts, could risk causing wireless providers to divert resources away from innovative solutions that can more accurately and effectively target spam text messages toward

[36] *See Petitions for Declaratory Ruling on Regulatory Status of Wireless Messaging Service*, Declaratory Ruling, 33 FCC Rcd 12075, 12095-97 ¶¶ 42-45 (2018) ("*Text Messaging Declaratory Ruling*").

[37] *See* CAC Report at 15-17; *see also supra* Section II.

[38] CAC Report at 6.

[39] *Id.* at 17.

fulfilling a regulatory mandate with no clear consumer benefit. For example, text messages sent by non-consumers without consumer consent violate industry best practices and may be blocked by wireless providers' spam filters or other tools. For this reason, the CAC recommended that the Commission "consider ways to encourage all industry stakeholders to employ CTIA's principles of requiring consent."[40]

The *Notice*'s proposal to require blocking of messages from "invalid" telephone numbers also does not grapple with *legitimate* wireless text messages that do not originate from a North American Numbering Plan ("NANP") telephone number, including messages originating from short codes,[41] OTT applications with internet end-points, including IP-addresses, and wireless provider-supported email-to-text messages.[42] The Commission should be cautious about preventing legitimate uses of text messaging that do not originate from a NANP telephone number.

[40] CAC Report at 19.

[41] The primary function of a short code is "effectively identical to the assignment of a Uniform Resource Locator (URL) to an entity wishing to set up a website. Just as a URL corresponds with a harder-to-remember IP address, a short code corresponds with more complex addresses, facilitating communication with the holder of the Short Code." *See* CTIA Opposition to Twilio Petition for Declaratory Ruling, WT Docket No. 08-7, at 32-34 (filed Nov. 20, 2015).

[42] *Text Messaging Declaratory Ruling*, 33 FCC Rcd at 12078 ¶ 9 ("The messaging ecosystem has evolved to include a variety of wireless messaging services and providers. Mobile service providers that offer wireless messaging service generally provide it as a native function on a mobile handset by using telephone numbers. But mobile service providers are not the only providers offering consumers the ability to send wireless messages. Applications providers like WhatsApp and Apple's iMessage also offer wireless messaging service. Generally, application providers offer wireless messaging service through apps that are downloaded from smartphone app stores. Some applications are used exclusively over the Internet and use IP addresses for routing. Others provide users with phone numbers that allow messages to be exchanged between telephone numbers and Internet endpoints.") (internal citations omitted).

Moreover, the text messaging ecosystem also presents a distinct set of issues with respect to regulatory classifications. In the voice context, Commission action was needed to clarify whether and when voice providers may block calls in light of common carrier nondiscrimination requirements and call completion rules that made the scope of voice providers' authority to block calls unclear.[43] Because wireless text messaging is not a Title II service, however, specific direction from the Commission regarding which messages to block and which to permit would be particularly inapt.[44]

Further, the *Notice*'s proposal to regulate criteria used by wireless providers to determine which text messages are "highly likely to be illegal" would be inconsistent with the classification of wireless messaging as Title I information service and raise First Amendment questions.[45] To enhance efforts to minimize erroneous blocking, legitimate message senders should be encouraged to adopt industry best practices, including CTIA's *Messaging Principles and Best*

[43] *See, e.g.*, *2017 Call Blocking Order*, 32 FCC Rcd at 9726 ¶ 60 (clarifying that call blocking consistent with the requirements adopted therein was permissible despite the requirements of 47 U.S.C. §§ 201-202); *see also id.* at 9709 ¶ 9 & n.28 (citing rural call completion rules at 47 C.F.R. § 64.2101 *et seq.*).

[44] Indeed, given that the Commission's call blocking rules for voice services—a service generally governed by Title II common carrier obligations—are largely *permissive*, it would be highly incongruous for the Commission to adopt *mandatory* blocking rules for text messaging, a Title I information service. The *Notice* provides no rationale for why a mandatory approach is warranted for wireless providers that are already blocking messages that do not originate from valid sources or with valid information. *Notice* ¶ 19; *infra* Section III.B.2. (discussing how the specific blocking rule in the *Notice* could undermine industry efforts to block texts based on more sophisticated criteria).

[45] *Text Messaging Declaratory Ruling*, 33 FCC Rcd at 12100 ¶ 48 & n.164.

Practices.[46] Wireless providers also have dedicated resources and solutions to the address concerns about erroneous blocking of legitimate text messages.[47]

Finally, the Commission has previously recognized that wireless service providers are not the only entities offering consumers the ability to send wireless messages.[48] Wireless messaging services are also supported by OTT applications that consumers use alongside SMS/MMS messaging. Some OTT applications are used exclusively over the Internet and use IP addresses for routing. Others provide users with telephone numbers that allow messages to be exchanged between telephone numbers and Internet endpoints.[49] As bad actors target consumers over SMS, they are also targeting consumers of OTT messaging applications, as noted above.[50] And, like wireless providers, OTT application providers have also introduced capabilities and features to protect consumers from spam.[51]

The Commission should refrain from pursing its proposal, and instead continue to allow messaging stakeholders to actively work to protect consumers using their sophisticated and ever-evolving blocking technologies and other solutions. Indeed, the Commission should encourage *all* messaging providers and others in the ecosystem to continuously innovate in order to prevent spam messages and deter bad actors from targeting the messaging platform. A regulatory

---

[46] *See* CAC Report at 19.

[47] Given these efforts, rules requiring providers to offer another point of contact or to respond to complaints within a specific period of time would be superfluous. *See Notice* ¶ 27.

[48] *See, e.g.*, *Text Messaging Declaratory Ruling*, 33 FCC Rcd at 12099 ¶ 47 & nn.158-159.

[49] *Id.* at 12078 ¶ 9; *Notice* ¶¶ 23, 33.

[50] *See, e.g.*, Bill Toulas, Massive Facebook Messenger phishing operation generates millions, BLEEPING COMPUTER (June 8, 2022), https://www.bleepingcomputer.com/news/security/massive-facebook-messenger-phishing-operation-generates-millions/.

[51] *See, e.g.*, WhatsApp About spam and unwanted messages, *supra* note 10; Facebook Messenger Blocking, reporting and deleting, *supra* note 10.

construct focused only on part of the messaging ecosystem will not discourage bad actors from targeting consumers.

2. The Caller ID Authentication Proposal Imported From the Robocall Playbook Does Not Apply to the Messaging Technology or Issues That Industry Is Already Addressing.

Mobile messaging networks already incorporate a substantial degree of authentication, and the wireless industry is working to improve its authentication capabilities today. As a result, a Commission mandate requiring wireless providers to "implement caller ID authentication for text messages"—particularly by mandating a particular solution such as STIR/SHAKEN—would be both unnecessary and counterproductive.[52]

As explained above, wireless messaging providers already incorporate a substantial degree of authentication to address the problems of bad actors legitimately using valid telephone numbers to originate spam text messages.[53] For example, wireless providers require non-consumer senders to work with registrars and aggregators to go through up-front vetting and registration to make sure they are who they say they are.[54] Further, the architecture of wireless messaging platforms is such that wireless providers already know the transmitting provider (e.g., wireless provider or messaging solutions aggregator) and user identifier (whether long code, short code, or other marker) for text messages. Wireless providers use this information to deliver text messages typically only from authorized providers and user identifiers using valid originating information through appropriate routing channels, and to more readily identify unauthorized traffic using illegitimate channels.

---

[52] *Notice* ¶¶ 30-31.

[53] *See supra* Section II.

[54] *See* CAC Report at 8-9, 16-17.

As a result, wireless providers have significantly more information about message senders than voice providers, they apply more sophisticated spam mitigation tools, and they are already working on making authentication in messaging even more effective. In the face of these efforts, a specific regulatory mandate to adopt a caller ID authentication solution is not needed and could suppress innovation to improve consumer protection.[55]

Moreover, the caller ID authentication solution proposed in the *Notice*, STIR/SHAKEN—is not applicable to the majority of text messages. The wireless industry led the way in developing the purpose-built STIR/SHAKEN call authentication standard for voice services and wireless providers have implemented it across their IP-based voice calling services, but STIR/SHAKEN is exclusively a SIP technology that does not apply to the majority of text messages (SMS, MMS and others), which are not sent using SIP.[56]

The IETF document referenced in the *Notice*[57] focuses on the small portion of use cases where text messages are handled on SIP networks.[58] It specifically notes that MMS messages are typically conveyed with Simple Mail Transfer Protocol ("SMTP") rather than SIP, and that the SMTP environment provides "a suite of additional email security tools … for sender authentication," but the "interaction of these mechanisms with STIR certificates and/or PASSporTs *would require further study and is outside the scope of this document*."[59] As to "other cases where messages are conveyed by some protocol other than SIP," the IETF

---

[55] *See, e.g.*, CTIA Messaging Security Best Practices.

[56] CAC Report at 3-4; *Text Message Declaratory Ruling*, 33 FCC Rcd at 12078-79 ¶¶ 8-11.

[57] *Notice* ¶¶ 13, 29, (citing IETF, *Messaging Use Cases and Extensions for STIR*, Draft, at 2-3 (2021), https://datatracker.ietf.org/doc/draft-ietf-stir-messaging ("IETF Draft Standard")).

[58] IETF Draft Standard §§ 3.1., 3.2.

[59] *Id.* at § 3.2.1 (emphasis added).

document offers only conjecture as to whether STIR/SHAKEN authentication processes could be applied.[60] Another technical standards body, the IP NNI, is beginning to consider additional authentication frameworks for more commonly used messaging formats and protocols.[61]

Technical and operational authentication solutions are being actively considered that may be able to complement the vetting and monitoring solutions in use today. But these efforts are in preliminary stages, and significant study is needed to explore the use of additional authentication measures for messaging. Rather than forcing the wireless messaging industry to adopt a technical solution for authentication that is not applicable to the issues or technology used by most text messaging, the Commission should encourage the wireless industry to continue evaluating potential technical and operational solutions to enhance authentication on text messaging networks.

IV. THE COMMISSION CAN BEST PROTECT CONSUMERS FROM UNWANTED AND ILLEGAL TEXT MESSAGES BY ENHANCING INFORMATION-SHARING CAPABILITIES, ENFORCING EXISTING RULES, AND SUPPORTING INDUSTRY EFFORTS.

To best protect consumers from illegal and unwanted text messages, the Commission should leverage the tools it has available to collaborate with the wireless industry and government partners to target and mitigate harms posed by bad actors, and to educate messaging ecosystem stakeholders and consumers on how to protect themselves and the platform from spam texts. These and other steps will be far more effective at targeting and mitigating the harms posed by bad actors than the proposals in the *Notice*.

---

[60] *Id*.

[61] ATIS, IP NNI Task Force, https://www.atis.org/industry-collaboration/ip-nni-task-force/ (last visited Nov. 9, 2022).

Expand Information Sharing. The Commission is uniquely situated to aid industry efforts to coordinate information sharing across the messaging ecosystem. For example, CTIA's *Secure Messaging Initiative* offers promising opportunities for the Commission to engage a clearinghouse that can facilitate sharing information about bad actors and their tactics among industry and government representatives.[62] In addition, the Commission's Enforcement Bureau should open the online web portal, adopted last year, that will enable private entities to submit information about suspected text message spoofing violations.[63]

Enforce Existing Rules. The FCC should enforce its TCPA and Truth-in-Caller-ID rules against message senders that use autodialers to send consumer unsolicited texts or that transmit or display misleading or inaccurate caller ID information with the intent to harm consumers.[64] It would be premature to conclude that "traditional enforcement remedies, standing alone, may not be sufficient deterrents"[65] before any significant enforcement activity in this area has been pursued. For cases where bad actors are using legitimate numbers to harm consumers, including through tactics such as imposter fraud, the Commission should engage in greater coordination with the FTC to bring enforcement actions.

Encourage Adoption of Industry Best Practices. As the CAC recommended, the Commission should evaluate whether and how to encourage broader adoption of industry best practices among messaging stakeholders.[66] Specifically, the CAC recommended that the

---

[62] *See* CTIA Secure Messaging Initiative, *supra* note 9.

[63] *See TRACED Act Portal Order*.

[64] 47 C.F.R. § 64.1604.

[65] *Notice* ¶ 15.

[66] CAC Report at 19.

Commission consider ways to encourage all industry stakeholders to employ CTIA's *Messaging Principles and Best Practices* and its strong emphasis on obtaining consumer consent and honoring consumer opt-out requests, as well as participating registries that enable providers to identify bad actors.[67] The Commission should also encourage stakeholders throughout the messaging ecosystem to use CTIA's *Messaging Security Best Practices*, which identify a number of activities that could threaten messaging security and offers steps that stakeholders could take to protect against and address those threats.[68]

Educate Consumers. The CAC also recommended that the Commission and other government partners, such as the FTC and state attorneys general, as well as other stakeholders, should increase efforts at consumer education.[69] These efforts should ensure that consumers are aware of unwanted messaging solutions and industry efforts,[70] including network and device-level message blocking tools, and how to report unwanted messages through 7726 (SPAM) or the new reporting solutions within native messaging applications support by wireless operating systems.

CTIA encourages the Commission to use these readily available capabilities and to collaborate with the wireless industry to target bad actors and take meaningful steps to protect consumers. This approach would allow the Commission to avoid the proposals in the *Notice* that

---

[67] *Id*.

[68] CTIA Messaging Security Best Practices.

[69] CAC Report at 19.

[70] *See, e.g.*, CTIA, Protecting You From Spam Text Messages, *supra* note 8.

are ill-suited for text messaging, as well as unnecessary questions regarding the scope of the Commission's authority.[71]

V. CONCLUSION.

CTIA and its member companies throughout the wireless industry share the Commission's commitment to protecting consumers against spam text messages. Enhanced coordination with industry and other government representatives to enhance enforcement against bad actors, as well as other opportunities discussed herein, will better achieve these goals than the proposals in the *Notice*, and the Commission should target its efforts on that basis.

Respectfully submitted,

/s/ Sarah Leggin

Sarah Leggin
Director, Regulatory Affairs

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, N.W.
Suite 600
Washington, D.C. 20036
(202) 736-3200

November 10, 2022

[71] For instance, the Commission has never relied upon Section 251(e) to regulate activities that make use of telephone numbers for purposes unrelated to the routing of voice traffic over the PSTN. *See, e.g.*, *STIR/SHAKEN Order* (authentication of voice calls); *2017 Call Blocking Order*, 32 FCC Rcd 9706 (blocking voice calls highly likely to be illegal); *Numbering Policies for Modern Communications*, Report and Order, 30 FCC Rcd 6839 (2015) (use of numbering resources by IP-based voice providers for voice calls). The scope of the regulations proposed in the *Notice* would also trigger new questions about the extent of Commission's Title III authority. *See, e.g., NBC v. U.S.*, 319 U.S. 190, 216 (1943) (Title III authority is "not to be interpreted as setting up a standard so indefinite as to confer an unlimited power.").