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

In the Matter of	)	
	)	
Targeting and Eliminating Unlawful Text Messages	)	CG Docket No. 21-402
	)	
	)	
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
	)	

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Sarah Leggin
Assistant Vice President, Regulatory Affairs

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

May 8, 2023

TABLE OF CONTENTS

I. INTRODUCTION & SUMMARY....1

II. THE WIRELESS INDUSTRY'S EFFORTS TO PROTECT CONSUMERS FROM SPAM TEXT MESSAGES ARE ROBUST AND EVOLVING. 4

III. THE *FNPRM*'S BLOCK-ON-NOTICE REQUIREMENT DIFFERS SIGNIFICANTLY FROM THE GATEWAY PROVIDER RULE AND SHOULD NOT BE APPLIED TO TEXT MESSAGING....7

IV. CALLER ID AUTHENTICATION SOLUTIONS WOULD NOT EFFECTIVELY ADDRESS THE MAIN SOURCES OF SPAM TEXT MESSAGES....12

V. CTIA SUPPORTS COMMISSION EFFORTS TO PURSUE BAD ACTORS CONSISTENT WITH ITS STATUTORY MANDATE. 15

VI. CONCLUSION. 17

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

In the Matter of	)	
	)	
Targeting and Eliminating Unlawful Text Messages	)	CG Docket No. 21-402
	)	
	)	
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
	)	

COMMENTS OF CTIA

CTIA[1] respectfully submits these comments in response to the Federal Communications Commission's ("Commission" or "FCC") Further Notice of Proposed Rulemaking ("*FNPRM*") attached to its March 17, 2023 Order in above-referenced proceedings seeking to protect consumers from illegal and unwanted text messages.[2]

I. INTRODUCTION & SUMMARY.

The record in this proceeding has made clear that the wireless industry and partners in the messaging ecosystem are committed to protecting consumers and the messaging platform from spam text messages. The wireless industry's multi-pronged solutions are designed to target the specific ways spam text messages risk reaching consumers. The mobile wireless industry has

[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; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order and Further Notice of Proposed Rulemaking, FCC 23-21 (rel. Mar. 17, 2023) ("*Order*" or "*FNPRM*," as appropriate).

made, and continues to make, significant investments in these efforts to protect consumers from unwanted messages while supporting innovative uses of messaging. For example, between 2015 and 2020, while messaging grew in popularity and the total volume of text messages roughly doubled, wireless providers blocked *ten times* the number of spam text messages, from an estimated 1.4 billion in 2015 to 14 billion in 2020.[3] And blocking is only part of the broader effort to stop bad actors at the source in order to protect consumers from spam text messages.

The wireless industry continues to evolve the playbook to successfully prevent billions of spam text messages from ever reaching consumers each year, particularly as bad actors continue to change their tactics. As the record in this proceeding demonstrates, the problems underlying text spam are different from those that underlie robocalls and demand different solutions.[4] As a result, the proposals in the *FNPRM*, which are drawn from the robocall environment, would do little to enhance existing industry efforts to reduce text spam or protect consumers.

Specifically, the Commission should refrain from extending the obligations on gateway voice service providers to investigate and block illegal robocall traffic based on notice from the Commission to terminating wireless providers. Terminating wireless providers' role in the messaging space is very different from the role of gateway voice service providers, and the policy rationale for the rule in the robocall context does not apply in the messaging ecosystem.

---

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

[4] Reply Comments of Fifty-One State Attorneys General, CG Docket No. 21-402, at 4 (filed Dec. 9, 2022) ("Over the last year, members of the Robocall Technologies Working Group have spoken with CTIA, the trade association for the U.S. wireless industry, as well as cloud-based provider Twilio, wireless provider Verizon, and others to learn more about the technological logistics and participating players of the messaging ecosystem. We understand from these productive conversations that, for several reasons, the messaging ecosystem and the voice call ecosystem are significantly different in infrastructure.") (footnote omitted).

In addition, new industry initiatives, such as CTIA's Secure Messaging Initiative, provide a more effective means for the Commission and industry to share information and harness the Commission's enforcement authority to target bad actors.

The Commission should also maintain the approach it correctly took in the *Order*, where it deferred its proposal to require providers to adopt a caller ID authentication solution for text messages because efforts to develop such solutions "are preliminary and require more study."[5] As the Commission observed in the *FNPRM*, the record in this proceeding shows that "illegal and unwanted messages rarely come from spoofed numbers and a caller ID authentication solution, even if feasible, would be unlikely to reduce unwanted and illegal text messages."[6] Nothing has changed since the *Order*'s adoption that would support a different result today. In fact, the record demonstrates that the *FNPRM*'s proposal to implement a caller ID authentication solution for text messaging would not be an effective solution to identify and block spam text messages.

In addition, the Commission's new robotexting mandatory blocking and point-of-contact rules are not even in effect yet; the Commission should gain experience with and consider the effectiveness of these new obligations before it explores further action.

Finally, the Commission is right to target bad actors using the Telephone Consumer Protection Act ("TCPA") and Truth in Caller ID rules. However, consistent with the recommendations of the Commission's Consumer Advisory Committee, the most effective and efficient way for the Commission to help guide text message senders and minimize spam text messages is to encourage broader adoption of CTIA's industry-leading best practices centered on

[5] *Order* ¶ 37.

[6] *FNPRM* ¶ 54 n.148.

consumer consent. To best protect consumers, the Commission should continue to expand its active cooperation with industry and other law enforcement agencies to target the bad actors.[7]

II. THE WIRELESS INDUSTRY'S EFFORTS TO PROTECT CONSUMERS FROM SPAM TEXT MESSAGES ARE ROBUST AND EVOLVING.

The record in this proceeding has demonstrated that wireless providers and their partners throughout the wireless messaging industry have been on the frontlines protecting consumers from spam text messages for decades. The wireless industry continues to enhance and evolve those efforts to keep pace with bad actors' ever-changing and increasingly complex tactics.

Wireless providers have invested enormous resources into systems and practices that protect consumers against spam text messages. To enhance transparency among message senders, messaging stakeholders have deployed up-front vetting, authentication-type practices, and traffic monitoring that support legitimate uses of messaging while also deterring bad actors from originating spam texts in the first place. Throughout the message flow, wireless providers and their partners offer a range of protections. For example, "AT&T employs a multi-layered defense against illegal and unwanted text messages that incorporates technological innovation and proactive collaboration."[8] Similarly, "T-Mobile employs sophisticated spam filtering software and account fingerprinting to identify and block spam text messages at the network level before they reach our subscribers. These spam filters are constantly tuned to detect spam text messages based on evolving tactics of bad actors, such as volume, complaints, and links to malicious websites."[9] And Verizon "uses a myriad of tools and techniques to protect our

[7] *See* FCC, Consumer Advisory Committee, *Report on the State of Text Messaging*, at 19 (Aug. 30, 2022) ("CAC Report").

[8] Reply Comments of AT&T, CG Docket No. 21-402, at 5 (filed Dec. 9, 2022) ("AT&T Reply Comments").

[9] Comments of T-Mobile USA, Inc., CG Docket No. 21-402, at 4 (filed Nov. 10, 2022) ("T-Mobile NPRM Comments").

customers from spam, including blocking messages identified as illegal; stopping text campaigns that are inconsistent with a text message service's terms and conditions; requiring organizations originating texts to follow industry best practices such [as] obtaining consent prior to sending texts; and offering consumers options to opt in or opt out of certain texts arriving via particular channels."[10]

The wireless industry complements these technical approaches with industry-leading guidance for message senders. Stakeholders throughout the messaging ecosystem have adopted CTIA's *Messaging Principles and Best Practices*, which were developed by the wireless messaging industry and are centered around consent. Specifically, the *Messaging Principles* encourage all Non-Consumer message senders to obtain consumer consent before sending messages. By doing so, the *Messaging Principles* help ensure consumers get only the messages they want to receive, and not those they don't. The Rural Wireless Association has noted that industry best practices, such as CTIA's, "have proven largely effective in combatting unwanted robotexts."[11] Twilio also "promotes adoption of industry best practices and collaborates with industry partners to maintain trust in the text messaging environment."[12] These efforts result in considerable protection for consumers, preventing billions of spam text messages from ever reaching consumers each year.[13]

[10] Comments of Verizon, CG Docket No. 21-402, at 2 (filed Nov. 10, 2022) ("Verizon NPRM Comments").

[11] Reply Comments of the Rural Wireless Association, Inc., CG Docket No. 21-402, at 4 (filed Dec. 9, 2022).

[12] Reply Comments of Twilio Inc., CG Docket No. 21-402, at 2-3 (filed Dec. 11, 2022).

[13] *See* Comments of CTIA, CG Docket No. 21-402, at 6-7 (filed Nov. 10, 2022) ("CTIA NPRM Comments").

More recently, CTIA launched the *Secure Messaging Initiative* ("SMI") to enhance public-private partnerships with law enforcement entities seeking to crack down on the bad actors that are behind spam texts.[14] The SMI has two components: 1) a *technical working group* to develop new tools and capabilities and 2) an *information-sharing working group and clearinghouse* to share information among providers in the texting ecosystem and partner with governmental enforcement agencies to identify and stop bad actors.

In the SMI Technical Working Group, technical and anti-fraud experts work together to identify how bad actors appear to be sending spam and develop best practices to address those specific tactics. A result of this work is CTIA's *Messaging Security Best Practices*, published last year, which offers guidance to all messaging stakeholders on how to protect the messaging platform from unwanted messaging that may result from techniques including email-to-text, snowshoe messaging, and compromised access credentials.[15] The group is continuing to track trends in spam text messaging and enhance or develop new recommendations on how stakeholders should mitigate those threats.

The SMI Information Sharing Working Group is a member-driven clearinghouse that identifies spam text message campaigns to refer to law enforcement partners for investigation. While wireless providers already work with law enforcement to take steps that prevent bad actors from reaching their subscribers, the Information Sharing Working Group is designed to accelerate and streamline these efforts through a central clearinghouse. CTIA was proud to recently launch pilot programs with the FCC's Enforcement Bureau and a state attorney

[14] *See* CTIA, *CTIA Secure Messaging Initiative*, https://www.ctia.org/ctia-secure-messaging-initiative (last visited May 8, 2023).

[15] *See* CTIA, *Messaging Security Best Practices* (June 2022), https://www.ctia.org/the-wireless-industry/industry-commitments/messaging-security-best-practices.

general's office to make its first referrals. These referrals can provide the basis for the Commission and state agencies to protect consumers by investigating and potentially pursuing enforcement action against the bad actors sending illegal text messages. CTIA looks forward to expanding on these efforts and building upon this public-private partnership with other industry partners and agencies to enhance enforcement efforts.

III. THE *FNPRM*'S BLOCK-ON-NOTICE REQUIREMENT DIFFERS SIGNIFICANTLY FROM THE GATEWAY PROVIDER RULE AND SHOULD NOT BE APPLIED TO TEXT MESSAGING.

The *FNPRM* seeks comment on a proposal to impose on "terminating mobile wireless providers" an obligation "to investigate and potentially block texts from a sender after they are on notice from the Commission that the sender is transmitting suspected illegal texts, similar to [its] requirement for gateway providers with respect to voice calls."[16] The *FNPRM* describes this proposal as "similar to" the Commission's requirements for gateway providers with respect to voice calls,[17] but the proposal differs from the gateway provider block-on-notification requirement in crucial respects—namely, there are significant "differences between calling and texting that would suggest that this model would not work well for texting."[18]

First, the key elements of the gateway provider robocall rules—knowing upstream providers, investigating suspected spam messages, and blocking where appropriate[19]—are already in place in the mobile messaging ecosystem thanks to the regulatory environment that allows flexibility and fosters innovation. Messaging stakeholders already "know their

[16] *FNPRM* ¶ 50.

[17] *Id*. ¶¶ 50-52, *citing* 47 C.F.R. § 64.1200(n)(5).

[18] *See FNPRM* ¶ 53.

[19] *See* 47 C.F.R. § 64.1200(n).

customers" through practices like up-front registration and vetting.[20] They also already investigate and block *billions* of messages annually, as noted above.[21] In addition, existing industry initiatives such as CTIA's SMI provide an opportunity for the Commission and industry to share information and use its enforcement authority against bad actor message senders.

In contrast, in the robocall context, due to voice service providers' common carrier obligations and expectations to complete all calls, the Commission needed to provide gateway providers direction to investigate and block upstream traffic.[22] Text messaging stakeholders do not need such direction or any Commission action to spur continued know-your-customer efforts, investigation, and blocking. As a result, the proposed mandate for messaging providers is unnecessary.

Even if there were a need for a text messaging rule "similar to [the Commission's] requirement for gateway providers with respect to voice calls,"[23] the *FNPRM*'s proposal differs significantly from the gateway provider rules in ways that undermine both its rationale and its effectiveness. Perhaps most significantly, the *FNPRM* proposes "to require *terminating* mobile wireless providers to investigate and potentially block texts from a *sender* after they are on notice from the Commission that the *sender* is transmitting suspected illegal texts."[24] By

[20] *See, e.g.*, Reply Comments of CTIA, CG Docket No. 21-402, at 3-7 (filed Dec. 9, 2022) ("CTIA NPRM Reply").

[21] *Id*. at 1.

[22] *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) (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*.).

[23] *FNPRM* ¶ 50.

[24] *Id*. (emphasis added).

contrast, the robocall block-on-notification rule applies to "gateway providers" that serve as the entry point for foreign voice calls onto U.S. telecommunications networks.[25] The *FNPRM* offers no explanation, but this difference is significant because both the *justification for* and the *mechanics of* the gateway provider rule depend on the particular role that gateway providers play in robocall traffic—which is unlike the role terminating wireless providers play in the text messaging ecosystem.

The Commission adopted the gateway provider rule based on a determination that foreign-originated calls were "a significant portion, if not the majority, of illegal robocalls" such that "gateway providers serve as a critical choke-point for reducing the number of illegal robocalls received by American consumers."[26] These findings provided a policy underpinning for the obligation on gateway providers to investigate suspected illegal robocalls, upon Commission notification, and to block calls or callers found to be originating robocalls.[27] These findings also established the foundation for the practical administrability of the rules: since gateway providers are the point of entry for foreign traffic into the U.S. with the ability and (per the *Gateway Provider Order*) duty to "know their upstream providers" overseas that might be originating illegal robocalls,[28] their ability both to identify potentially illegal traffic and to block it are readily apparent from the circumstances.

---

[25] 47 C.F.R. §§ 64.1200(f)(19), (n)(4).

[26] *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, Sixth Report and Order in CG Docket No. 17-59, Fifth Report and Order in WC Docket No. 17-97, Order on Reconsideration in WC Docket No. 17-97, Order, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 22-37, ¶¶ 23-24 (rel. May 20, 2022) ("*Gateway Provider Order*").

[27] *Id*. ¶¶ 74-75.

[28] *Id*. ¶¶ 96-101.

Imposing similar requirements on terminating mobile wireless providers for robotexts, however, could not be supported by similar policy rationales and would raise different practical problems. Unlike gateway providers for foreign voice calls, a terminating mobile wireless provider delivering text messaging traffic to subscribers is not serving as a "critical choke-point" with respect to potentially illegal traffic the way gateway providers are.[29] As the Commission's Consumer Advisory Committee noted, there are several major types of entities that play key roles in originating and transmitting text messages to consumers, including cloud-based providers and aggregators for example,[30] and there is no basis in the record to even analyze which of them might be in a position analogous to gateway providers. Likewise, the practical considerations involved in requiring terminating wireless providers to investigate and block potentially illegal messages coming from upstream providers are different from those involved in imposing similar obligations on international gateway voice providers. This is true for a variety of reasons, including the ever-evolving tactics used by bad actors to send spam text messages (e.g., brand impersonation, SIM boxes, snowshoe messaging, etc.).[31] The *FNPRM* does not acknowledge these considerations and includes no proposed rule language to illuminate how the Commission would address them.[32]

---

[29] *Id*. ¶ 24.

[30] CAC Report at 8-9 (stating "Cloud-Based Providers that enable non-consumers to send messages, among other communications services, through internet-based portals and applications over various channels to be delivered to consumers" and "Aggregators that facilitate the flow of non-consumer messaging traffic from the cloud-based provider systems to each mobile wireless network.").

[31] *See, e.g., id*. at 11.

[32] *See Order* and *FNPRM* at App. C. As just one example, the *FNPRM* does not explain how the Commission would define a "sender" of potentially illegal text messages for purposes of the proposed blocking rule. *See FNPRM* ¶ 50.

Given these challenges, if the Commission wishes to play a more active role in helping to identify and block text spam, a more constructive approach would be to engage directly with mobile wireless providers' ongoing efforts.[33] In particular, providers and government agencies can leverage CTIA's SMI central clearinghouse to share information about suspected spam text messages and the bad actors behind them.[34] To the extent that the Commission obtains information about senders or types of text messages that may be illegal, the Commission can bring them to the SMI clearinghouse, where they will be shared with participating actors in the text messaging ecosystem that are in a position to stop text spam. The goal of this clearinghouse, and the SMI more broadly, is to "rapidly and effectively shut down spam activity and help enforcement agencies target bad actors that send unwanted or fraudulent messages."[35] This is consistent with the goals of the Commission's blocking proposal, but the SMI would provide a more effective way to achieve it.

If the Commission nevertheless adopts rules applicable to mobile wireless text messaging providers, it should rely on the same sources of authority that it relied upon to adopt the *Order*—in particular, the TCPA and Truth in Caller ID Act.[36] As the Commission concluded in the

[33] Comments of the High Tech Forum, CG Docket Nos. 21-402 & 02-278, at 2 (filed Apr. 16, 2023) ("Text messaging is different from phone calls because it doesn't require manual acceptance of each communication. Text messaging is different from email spam because the originating party is nearly always whoever they claim to be. But just as spam blocking depends on rapidly learning the sources and content of unwanted messages, spam text blocking depends on detecting messages that can be sent from a variety of names or numbers. Both are exercises in information sharing.")

[34] CTIA, *CTIA Secure Messaging Initiative*, https://www.ctia.org/ctia-secure-messaging-initiative (last visited May 8, 2023).

[35] *Id.*

[36] *Order* ¶¶ 38-40.

Order, because these authorities "provide sufficient authority" over text message spam, it is "unnecessary to address other possible sources of authority."[37]

IV. CALLER ID AUTHENTICATION SOLUTIONS WOULD NOT EFFECTIVELY ADDRESS THE MAIN SOURCES OF SPAM TEXT MESSAGES.

As the Commission correctly observes in the *FNPRM*, the record in this proceeding shows that "illegal and unwanted messages rarely come from spoofed numbers and a caller ID authentication solution, even if feasible, would be unlikely to reduce unwanted and illegal text messages."[38] Nevertheless, the *FNPRM* seeks comment on "the extent of number spoofing" in the text messaging context and how the Commission might "encourage industry members to collaborate and finalize technical solutions for authenticating text messages."[39]

As the record in this proceeding amply shows, "spoofing is not a significant problem in text messaging."[40] "Rules addressing spoofed texts would not protect consumers because there is no spoofing problem to fix."[41] As an international messaging association noted, while "spoofed-number security incidents have been reported (e.g., 'sent from my own number' spam campaigns as reported in the press)," service providers' internal originating number

[37] *Id*. ¶ 40. For example, as CTIA has previously discussed, attempting to rely on Section 251(e) would raise unnecessary questions about the scope of the Commission's authority, given that text messaging is an information service. *See* CTIA NPRM Comments at 21 & n.71.

[38] *FNPRM* ¶ 54 n.148.

[39] *Id*. ¶ 54.

[40] Comments of the Messaging Malware Mobile Anti-Abuse Working Group, CG Docket No. 21-402, at 15 (filed Nov. 8, 2022) ("M^{3}AAWG NPRM Comments"); *see also* T-Mobile NPRM Comments at 8-9; Comments of the Blooston Rural Carriers, CG Docket No. 21-402, at 2-3 (filed Nov. 10, 2022); Comments of Campaign Verify Inc., CG Docket No. 21-402, at 3-6 (filed Nov. 10, 2022) ("Campaign Verify Comments"); Comments of Telesign, CG Docket No. 21-402, at 2 (filed Nov. 8, 2022); Comments of WMC Global, CG Docket No. 21-402, at 1-2 (filed Oct. 21, 2022) ("WMC Global Comments"); Reply Comments of Verizon, CG Docket No. 21-402, at 1 & 4 (filed Dec. 9, 2022); Reply Comments of NetNumber, Inc., CG Docket No. 21-402, at 2 (filed Dec. 9, 2022) ("NetNumber Reply Comments").

[41] Verizon NPRM Comments at 6.

authentication process are "rarely-defeated" and, as a result, a caller ID authentication process "would be no more effective in empowering blocking than existing anti-spoofing mechanisms."[42] Further, the record makes clear that brand impersonation and social engineering tactics to take over *legitimate* message sender accounts are the predominant means of producing spam text messages.[43]

The record also shows that "the wireless industry is engaged in sophisticated, resource-intensive efforts to curb unwanted messaging," through approaches tailored to address those issues unique to text messaging.[44] As noted above, up-front vetting and registries provide a first line of defense, stopping bad actors who cannot demonstrate legitimate uses for high-volume messages and providing information that providers can use to take swift action if spam is discovered.[45] Enforcement of industry best practices centered around consumer consent, along with on-going monitoring procedures (e.g., pattern analysis, "honeypot" spam lures), blocking of spam messages, and other industry tools further enable wireless providers to stop illegal texts at the source and on-network.[46] On the back end, complaints from consumers (submitted to 7726 ("SPAM") or via mobile operating system-based solutions (e.g., "Report Junk")) provide the

[42] M^{3}AAWG NPRM Comments at 14-15. *See also FNPRM* ¶ 54 & n.150 (citing a single example of a commenter alleging text message spoofing).

[43] *See, e.g.*, AT&T Reply Comments at 10; Reply Comments of the Cloud Communications Alliance, CG Docket No. 21-402, at 1-3 (filed Dec. 9, 2022); Reply Comments of INCOMPAS, CG Docket No. 21-402, at 5 (filed Dec. 11, 2022); NetNumber Reply Comments at 2-3; M^{3}AAWG NPRM Comments at 10-11; WMC Global Comments at 1 & 5; Comments of the Professional Associations for Consumer Engagement, CG Docket No. 21-402, at 1-2 (filed Nov. 10, 2022); Campaign Verify Comments at 6-7.

[44] Letter from Scott Bergmann, Senior Vice President, Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 21-402 & 02-278, at 2 (filed Mar. 7, 2023). *See also* CTIA NPRM Reply at 3-7 (summarizing the record).

[45] *See supra* Section II.

[46] *See, e.g.*, CTIA NPRM Reply at 5-6.

next level of deterrence that enables providers to quickly identify and block spam text messages.[47] Finally, CTIA's SMI offers a new tool in the toolbox that will enable the wireless industry to partner with law enforcement agencies to crack down on bad actors using brand impersonation and account hijacking to send spam texts.

In the *Order*, the Commission correctly deferred its proposal to require providers to adopt a caller ID authentication solution for text messages because efforts to develop such solutions "are preliminary and require more study."[48] Nothing has changed since the *Order*'s adoption that would support a different result today.

As the record reflects, the wireless industry continues to evaluate new technical and operational solutions.[49] For example, the Alliance for Telecommunications Industry Solutions' ("ATIS") IP-NNI Task Force is exploring the text messaging landscape, stakeholders, architectures, available spam mitigation tools, and the sources of spam text messages to determine whether new technical or operational standards should be explored to mitigate those threats. The Commission should continue to encourage these and other industry-driven efforts that may yield solutions to further mitigate spam text messages and complement other industry solutions. Because no single solution for text message authentication exists today, the cost of complying with such an obligation would be considerable and difficult to estimate. This further militates against such an obligation at this time.

[47] *See, e.g.*, M[3]AAWG NPRM Comments at 4; Comments of Sinch America, Inc., CG Docket No. 21-402, at 10 (filed Nov. 10, 2022).

[48] *Order* ¶ 37.

[49] *See, e.g.*, CTIA NPRM Reply at 11.

Finally, the *FNPRM*'s question about how the Commission can ensure non-discriminatory policies in adopting text authentication measures is a solution in search of a problem.[50] Surveys demonstrate that consumers object to unwanted messages regardless of the source.[51] Wireless providers share that view and are transparent about their messaging policies to protect consumers from all forms of spam text messages. For example, CTIA's *Messaging Principles and Best Practices* and providers' own published messaging policies describe the practices applied objectively across the ecosystem, regardless of the source or content of messages.[52] And the "point of contact" rule in the *Order* addresses commenters' concerns about legitimate messages being blocked. The Commission should, at least, assess the success of that rule before considering any additional action.[53]

V. CTIA SUPPORTS COMMISSION EFFORTS TO PURSUE BAD ACTORS CONSISTENT WITH ITS STATUTORY MANDATE.

The *FNPRM* proposes to clarify that the Commission's existing Do Not Call rules apply to text messages, consistent with the Commission's 2003 determination that text messages are "calls" for purposes of the TCPA, and to close the "lead generator loophole" in the definition of "consent" in the Commission's Do Not Call rules, applicable to both calls and text messages.[54]

---

[50] *FNPRM* ¶ 54.

[51] *See* CTIA, *Keeping Consumers Spam Free During Election Season*, CTIA Blog (Sept. 22, 2022), https://www.ctia.org/news/keeping-consumers-spam-free-during-election-season.

[52] *See* CTIA, *Messaging Principles and Best Practices* (July 2019), https://www.ctia.org/the-wireless-industry/industry-commitments/messaging-interoperability-sms-mms. *See also* CTIA NPRM Reply at 5-6 (discussing and citing wireless providers' policies).

[53] The text messaging ecosystem presents a distinct set of issues with respect to regulatory classifications. Because wireless text messaging is not a common carrier service, specific direction from the Commission regarding which messages to block and which to permit in a "non-discriminatory" manner would be particularly inapt. The Commission should avoid unnecessary questions about whether it has authority to adopt such a proposal.

[54] *FNPRM* ¶¶ 55-62.

As CTIA has noted previously in this proceeding, the TCPA and the Truth in Caller ID Act provide the Commission with authority to pursue action directly against such bad actors,[55] and CTIA supports the Commission taking action against bad-actor message senders consistent with this authority.[56]

While the TCPA rules provide baseline protections for consumers against bad actors, CTIA's *Messaging Principles and Best Practices* already offer stronger, clearer protections from unwanted messages. The *Messaging Principles and Best Practices* are based on the TCPA's central tenet of consent before senders can contact consumers, and they clarify that all non-consumer messages should have consent before sending messages. For example, the *Messaging Principles and Best Practices* already offer guidance on the importance of obtaining consumer consent to a specific campaign before sending text messages:

- Section 5.1 says that the "consumer should give express written permission before a business sends them a text message."
- Section 5.1.4 discourages renting, selling, or sharing of "opt-in" lists and encourages message senders to create and vet their own opt-in list.

For these reasons, regardless of whether the FCC adopts the *FNPRM*'s proposals, the Commission should follow through on the Consumer Advisory Committee's recommendation that the Commission "encourage all industry stakeholders to employ CTIA's principles of requiring consent."[57] Broader adoption of the *Messaging Principles and Best Practices* is the most effective and efficient way to minimize spam text messages.

---

[55] CTIA NPRM Comments at 20; CTIA NPRM Reply at 14-16.

[56] The Commission should make clear that the obligations, consistent with the TCPA, apply to message senders. While wireless providers will continue to support the *Messaging Principles and Best Practices*, wireless providers are not and should not be obligated, as a matter of law, to act as an enforcement agent with respect to the TCPA laws and rules applicable to message senders.

[57] CAC Report at 19.

VI. CONCLUSION.

The wireless industry is dedicated to protecting consumers from spam text messages and seeks collaboration among multiple entities throughout the messaging ecosystem, as well as government and law enforcement agencies, including the Commission, to do so. Rather than pursue proposals to superimpose robocall solutions onto the text messaging ecosystem, which presents significantly different technical and policy considerations, the Commission should focus its efforts on enhancing coordination with industry and other government representatives to take action against bad actors. These efforts will better achieve the Commission's goals to protect consumers from spam text messages.

Respectfully submitted,

/s/ Sarah Leggin

Sarah Leggin
Assistant Vice President, 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

May 8, 2023