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 INCOMPAS

INCOMPAS submits these comments in response to the Federal Communications Commission's ("Commission") *Notice of Proposed Rulemaking* seeking comment on proposals to require mobile wireless providers to block illegal texts at the network level and to apply caller ID authentication standards to text messaging.[1]

I. INTRODUCTION & SUMMARY

Like illegal robocalling, unlawful text messaging significantly increases the risk of fraud for consumers and threatens user confidence in this popular form of communication. INCOMPAS and its members, which have dedicated significant time and resources to mitigating illegal robocalls, appreciate the opportunity to address the Commission's proposals to target illegal robotexting. Protecting consumers from illegal robotext campaigns and preserving a competitive texting environment is a top priority for INCOMPAS members whose customers use text messaging for many legitimate uses, including notification and verification. INCOMPAS believes that the Commission can play an important role in ensuring that consumers are not defrauded by bad actors while maintaining a competitive marketplace for providers engaged in

[1] *Targeting and Eliminating Unlawful Text Messages,* Notice of Proposed Rulemaking, CG Docket No. 21-402, FCC 22-72 (rel. Sep. 27, 2022) ("*Notice*" or "*NPRM*").

text messaging. As the Commission addresses the growing problem of illegal robotexting, there may be lessons in the robocalling context that can inform solutions for robotexting, although it is important to recognize that there are differences between voice and text that may warrant different approaches to resolving the issue. Ultimately, any rules adopted must be applied only where the FCC has appropriate jurisdiction and in a competitively-neutral and non-discriminatory manner that preserves competition.

This approach will be important because in the current environment of text messaging, INCOMPAS and its members are concerned that competitive interests are not being well served by the arbitrary messaging framework in the mobile wireless industry that has taken root without any regulatory oversight. Specifically, our members have taken issue with certain aspects of wireless carriers' use of existing methods to block and mitigate unlawful robotexts. Before taking action, INCOMPAS urges the Commission to conduct additional fact-finding and data collection, first, on the magnitude of the illegal robotexting problem and, second, on concerns related to the methods used by the wireless industry to contain illegal robotexting.

Additionally, the STIR/SHAKEN standard was not developed for text messaging and is therefore not readily applicable to the authentication of text messages. A new, competitively neutral industry standard, specifically tailored to the robotexting context, will need to be developed for text messaging and INCOMPAS urges the Commission to seek further comment on the standard when it is released. Developing a valid set of industry specifications and protocols for messaging traffic routing and identification will advance consumer protections and consumer demand for effective messaging services concurrently. Tipping the balance entirely in the direction of effectively preventing competitive service offerings in the name of consumer protection is not a public policy that serves the public interest.

Finally, INCOMPAS argues that the analytics being used in the robocall context (which incorporates caller ID authentication) continues to block legitimate traffic and therefore should not be reflexively used to address unlawful robotexting.

II. CURRENT INDUSTRY METHODS TO MANAGE ILLEGAL ROBOTEXTING IN THE MESSAGING ECOSYSTEM HAVE CREATED HARMS TO COMPETITION AND INNOVATION

The wireless industry has developed the 10 Digit Long Code ("10DLC") framework for Application to Person ("A2P") text messaging and have incorporated rules and requirements that carriers may invoke at will. Providers that wish to engage in SMS messaging campaigns are required to register these campaigns with The Campaign Registry and are required to follow industry best practices and guidelines.[2] However, some of the wireless carriers' methods, like The Campaign Registry, carry significant operational burdens, privacy concerns, and high costs, but with little demonstrable consumer value being added. Public advocacy groups have asked the wireless industry to lift "recently-implemented limits and throttling as well as excessive filtering of P2P ["person-to-person"] messaging."[3] Additionally, our members indicate that the mobile operators and their chosen vendors that administer such A2P function like The Campaign Registry are free to impose fees for a myriad of registries and "compliance" penalties that mobile operators themselves do not pay, degrade competitors' products through blocking, and collect

[2] *See The Campaign Registry Explained*, THE CAMPAIGN REGISTRY, https://www.campaignregistry.com/what-is-campaign-registry/ (last visited Nov. 9, 2022).

[3] See *About Us*, COALITION FOR OPEN MESSAGING, https://www.coalitionforopenmessaging.org/ (last visited Nov. 9, 2022). In August, INCOMPAS proposed an amendment to the Consumer Advisory Committee's recently adopted Report on the State of Text Messaging that sought an acknowledgement that a number of advocacy groups had expressed concerns that the 10DLC framework hampers these groups' ability to engage in outreach using P2P texting, however, the Committee turned down the amendment. *See generally*, FCC, Consumer Advisory Committee, Report on the State of Text Messaging (2022).

sensitive information about their competitors' customers without any methods for recourse.[4] Call blocking behaviors, together with high costs mandated via the "registration framework," and the mandated sharing of customer data that exists in the 10DLC environment are not in consumers' best interests and disadvantage competitive providers seeking to interoperate to provide competitive messaging services that consumers want and demand.[5]

Ensuring a competitively neutral landscape is similarly critical to the work to protect consumers from illegal robotexting. The Commission has a history of ensuring that providers in concentrated markets could not use their control to harm or limit competition in upstream markets. CPNI restrictions, which were incorporated into the 1996 Act, offer one example. Before issuing any rules that would require network-level text blocking or apply caller ID authentication requirements, INCOMPAS urges the Commission to gather more facts to understand how the current framework and registration tools are working, whether they are serving competitive interests, and how best to improve the consumer experience. Additionally, the Commission should gather more precise, multi-sourced data about the magnitude of the illegal robotexting problem. Unlike the robocalling environment, there are tools that consumers can employ to address unlawful or unwanted robotexts. The Commission should collect

[4] *See* CSP Portal Guide, *The Campaign Registry*, https://www.campaignregistry.com/wp-content/uploads/TCR-guide.pdf (last visited Nov. 10, 2022) (explaining how to register "brands" or customers seeking to engage in robotext campaigns). Campaign Service Providers ("CSPs") are required to submit detailed information about their customers or "brands," which can be particularly sensitive given that some large mobile operators are launching services (e.g., CPaaS) that compete directly with CSPs that must disclose their customers details.

[5] *See, e.g.*, Cale Guthrie Weissman, *School communication app Remind blasts Verizon over SMS spam fee*, FAST COMPANY (Jan. 14, 2019), https://www.fastcompany.com/90291884/verizon-blasted-by-school-communication-app-remind-over-sms-spam-fee (explaining Verizon's efforts to combat digital spam through the implementation of a new fee on platforms that send SMS messages, including educational service Remind which allows educators to send notifications to students and families).

information about the existing tools to combat robotexts, which are currently available to individuals through their devices, software, and SMS providers. For example, most commercially-available smartphones allow you to block all unknown senders (by sending them to a special folder), to block specific numbers (*e.g.*, ones that might be harassing you), or to silence a text thread.

The wireless industry continues to insist that it is successfully managing robotexting, but neglect to recognize the severe lack of competitive neutrality that accompanies its management structure. Commission oversight may be necessary to ensure that efforts purportedly designed to combat robotexting are developed and implemented without harming competition. Seeking key additional information will inform the Commission's decision-making process and ensure that any new requirements imposed by the Commission address gaps or discriminatory behavior in the current framework.

III. THE COMMISSION SHOULD EXERCISE CAUTION BEFORE MANDATING TEXT BLOCKING

To address the issue of unlawful robotexting, the Commission first proposes to extend mandatory blocking protections used to mitigate illegal robocalls to text messages. While INCOMPAS takes no position on the Commission's proposal to allow providers to engage in network-level blocking of texts from invalid, unallocated, unused, or do-not-originate ("DNO") numbers, the Commission should not reflexively impose a mandate to block texts that appear to come from spoofed numbers. INCOMPAS remains concerned about blocking of legitimate calls in the robocall context, and the employment of similar blocking mechanisms for texting could have severe consequences, particularly without any identified, competitively-neutral redress mechanisms.

Again, looking at the robocall context, despite advancements, analytics for voice traffic can still be imprecise, causing legitimate voice calls to be mischaracterized or mislabeled as spam, or blocked. Recognizing that legitimate calls can still be degraded or blocked using analytics, carriers' analytics partners in some instances are offering providers the opportunity to pay them to have their numbers whitelisted and not blocked. This approach would do little to prevent unlawful robotexting, but could be interpreted as a "pay to robotext" scheme, compounding the competitive concerns discussed above. For providers that have had legitimate traffic blocked or mislabeled, blocking on the basis of analytics has degraded the reliability of the voice network, and INCOMPAS remains concerned that it would also degrade the texting environment for competitors if allowed to be further extended there.

Furthermore, from a consumer protection standpoint, text messaging enjoys a number of advantages compared to illegal robocalls that mitigate the need for mandatory blocking of robotexts. The Commission's approach should reflect those differences. First, voice service—particularly traditional landline service—does not always offer the self-blocking and filtering options on a call-by-call or number-by-number basis that text messaging does, particularly when received over a landline. Second, voice service is immediate. In contrast, text messaging consumers are afforded time to review and consider a text message before responding to it (if at all). Finally, text messaging does not have a method of indicating "spam likely" as voice does; rather it offers a more binary choice of whether to block the text or not (although some operating systems permit silencing of texts from a number if not outright blocking).

Should the Commission allow network-level blocking of robotexts, INCOMPAS agrees that the tools that service providers use to determine whether a text is highly likely to be illegal must be applied in a non-discriminatory, competitively, and content-neutral manner. More

transparency into the 10DLC process in this regard would also be valuable to competitive providers.

Furthermore, if the Commission does adopt blocking mandates for industry, INCOMPAS contends that those rules would not extend to over-the-top ("OTT") messaging services based on the current definition of "text message" in the Commission rules. In the *Notice*, the Commission asks whether such a mandate should include some or all OTT applications delivered over IP-based mobile data networks and whether the Commission's current definition of "text messages" would apply to OTT messages sent to wireless telephone numbers, but not to OTT messages sent to other users within the same application.[6] INCOMPAS posits that number-independent OTT messaging services—i.e., OTT messaging services that do not use numbers for routing decisions—do not fall within the statutory definition and are therefore out of scope for any mandate. The relevant statute covers services that connect to the PSTN either through voice (including POTS or interconnected VoIP) or text (i.e., SMS or successor technologies). The statute does not apply to OTT messaging services that do not connect to the PSTN through SMS. For these reasons INCOMPAS believes the Commission lacks the authority to include number-independent OTT messaging services in the proposed rules.

IV. THE COMMISSION SHOULD NOT REQUIRE A CALLER ID AUTHENTICATION SOLUTION FOR TEXT MESSAGING UNTIL A STANDARD IS FINALIZED AND THE COMMISSION HAS AFFORDED THE OPPORTUNITY FOR PUBLIC COMMENT

Finally, the Commission seeks comment on whether to require providers to implement caller ID authentication for text messages.[7] In the robocalling context, the STIR/SHAKEN

[6] *See Notice* at para. 33.

[7] *See Notice* at para. 28.

framework requires an originating voice service provider to share what it knows about the caller ID information transmitted with a call. The use of this framework is a key part of the Commission's efforts to combat illegal robocalls, and INCOMPAS remains encouraged that the framework, when fully deployed, will serve as a critical component of the Commission's and industry's efforts to mitigate illegal robocalls and prevent customers from being victimized by illegal spoofing. While a caller ID authentication solution for text messaging could be valuable, the Commission should not mandate a technological solution for applying such authentication to robotexts until a standard is finalized and released.

STIR/SHAKEN provides a model of automated and standardized solutions for caller ID authentication for voice calls, particularly when combined with improved redress measures.[8] However, as the Commission acknowledges in the *Notice*, the current STIR/SHAKEN standard is not currently usable with text messages.[9] While INCOMPAS appreciates the work that the Internet Engineering Task Force is undertaking to determine whether components of the STIR/SHAKEN framework can be applied to text messaging, the Commission should not impose such a requirement while the standard is still in development and before industry has the opportunity to review and provide feedback on any proposed standard.

INCOMPAS submits that the Commission's attempts to require industry to adopt response codes for immediate call blocking notification may be instructive in this proceeding. In

[8] In the robocalling context, voice service providers that block calls based on an analytics program are required to transmit an appropriate response code— specifically, SIP Codes 603, 607, and 608 for a call terminating on an IP network—to the origination point of the call and must include sufficient information in the header of the response code for a provider to seek redress for an erroneously blocked call. *See* 47 C.F.R. § 64.1200(k)(9)(i).

[9] *See Notice* at para 29.

the Commission's *Call Blocking Fourth Report and Order*, the Commission specified that a terminating voice service provider that blocks calls return SIP Codes 607 and 608 as a means of providing actionable information that allows voice service providers to seek redress if necessary.[10] At the time, these response codes had not been finalized or released by industry standards-making organizations. Industry subsequently reported that aspects of the Commission's *Order* would be technically burdensome and that compliance could more easily be achieved in the short term by making changes to the standard for SIP Code 603.[11] USTelecom successfully petitioned the Commission to add SIP Code 603 to the Commission's list of response codes in the agency's *Call Blocking Sixth Report and Order*.[12] This new call blocking notification standard, SIP Code 603+, was released in August and providers have begun to utilize this response code when blocking calls.[13]

If the data indicates that the magnitude of the problem warrants a technological response, the Commission can and should refer the issue to the North American Numbering Council and encourage industry standards organizations such as ATIS to develop a solution, and request

---

[10] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-69, Fourth Report and Order, 35 FCC Rcd 15221, 15240, para. 56 (2020) (to be codified at 47 C.F.R. § 64.1200(k)(9)(i)).

[11] *See* Letter from Joshua M. Bercu, Vice President, Policy & Advocacy, USTelecom to Marlene Dortch, Secretary, Federal Communications Commission, CG Docket No. 17-59 (filed Jul. 27, 2021)

[12] *See Advanced Methods to Target and Eliminate Unlawful Robocalls – Petition for Reconsideration and Request for Clarification of USTelecom—The Broadband Association*, CG Docket No. 17-59, Order on Reconsideration, Sixth Further Notice of Proposed Rulemaking, and Waiver Order, FCC 21-126, para. 12 (2021).

[13] *See* Press Release, Alliance for Telecommunications Solutions, ATIS/SIP Forum Innovation Delivers Robocall Call Blocking Notification Standard (Aug. 23, 2022), *available at* https://www.atis.org/press-releases/atis-sip-forum-innovation-delivers-robocall-call-blocking-notification-standard/.

periodic reports on progress. Once a standard is developed, the Commission should review it to determine whether it would be in the public interest to adopt it in some form, and must allow for comment on the Commission's record prior to adopting it.

Furthermore, the Commission seeks comment on the scope of any implementation mandate for authentication for text messages and whether any implementation mandate should include some or all OTT applications delivered over IP-based mobile data networks.[14] INCOMPAS contends that any requirement for providers to implement caller ID authentication for text messages would not extend to number-independent OTT messaging services based on the current statutory definition of "text message." As noted above in our discussion on mandatory text blocking, INCOMPAS believes the Commission lacks the authority to include number-independent OTT messaging services in the proposed rules.

V. CONCLUSION

For the reasons stated herein, INCOMPAS urges the Commission to consider the recommendations in its comments as it examines the issues raised in the *Notice*.

Respectfully submitted,

INCOMPAS

/s/ Christopher L. Shipley

Christopher L. Shipley
Attorney & Policy Advisor
INCOMPAS
1100 G Street NW, Suite 800
Washington, D.C. 20005
(202) 872-5746
cshipley@incompas.org

November 10, 2022

[14] *See Notice* at para. 33.