

**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 INCOMPAS**

INCOMPAS submits these comments in response to the Federal Communications Commission’s (“Commission”) *Further Notice of Proposed Rulemaking* seeking comment on additional proposals to protect consumers against illegal robotexts.<sup>1</sup>

INCOMPAS, the internet and competitive networks association, commends the Commission for taking action to provide “a baseline level of consumer protection from spoofed text messages” in its recent *Report and Order* and welcomes the opportunity to examine additional proposals that would mitigate the threat of illegal text messaging.<sup>2</sup> Preserving this important service from fraud is a top priority for INCOMPAS members whose business customers use text messaging for notification and verification, among other things. INCOMPAS believes that the Commission can play an important role in protecting consumers from illegal

---

<sup>1</sup> *Targeting and Eliminating Unlawful Text Messages, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 21-402, CG Docket No. 02-278, Report and Order and Further Notice of Proposed Rulemaking, FCC 23-21 (rel. Mar. 17, 2023) (“*Further Notice*” or “*FNPRM*”).

<sup>2</sup> See *FNPRM* at para. 48.

robotexting while simultaneously establishing a regulatory framework that extends the non-discriminatory and competitively neutral treatment it has applied in the call blocking context to voluntary text blocking.

In this proceeding, INCOMPAS has expressed concerns regarding the competitive implications of the voluntary messaging framework in the mobile wireless industry that has taken root without any regulatory oversight. If the Commission is going to meaningfully address robotexting, it must examine and correct for market distortions in this messaging framework that already are present. The current messaging environment carries significant operational and economic burdens, especially for smaller companies (including a myriad of registries and “compliance” obligations and related fees and penalties), as well as privacy concerns, such as the collection of sensitive information about their competitors’ customers without any methods for recourse.<sup>3</sup> In the absence of standardized, competitively neutral rules, the current dynamics create perverse incentives that allow gamesmanship and arbitrage schemes as well as fraudulent behaviors to thrive. Furthermore, the current framework is not well suited to marketplace solutions that will allow industry to universally resolve text messaging issues. Even Commission guidance on Telephone Consumer Protection Act (“TCPA”) behaviors is deemed irrelevant in the ecosystem as currently constructed.

For example, the Consumer and Governmental Affairs Bureau’s recently adopted a *Declaratory Ruling* that enables federal and state governmental agencies to make Medicaid enrollment calls and send text messages without violating robocall and robotext prohibitions.<sup>4</sup>

---

<sup>3</sup> See Comments of INCOMPAS, CG Docket No. 21-402, 3-5 (filed Nov. 10, 2022).

<sup>4</sup> See *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, U.S. Department of Health and Human Services *Petition for Declaratory Ruling*, CG Docket No. 02-278, Declaratory Ruling, DA 23-62 (rel. Jan. 23, 2023).

Our members serve some of the agencies that were trying to redetermine the eligibility of over 90 million Americans in Medicaid by the time the pandemic emergency period ended in May. Medicaid beneficiaries that were still eligible but unable to be contacted risked losing coverage, putting them in both health and financial risk. As the Commission acknowledged via its ruling, texting could help ensure these individuals remained enrolled in critical health coverage for which they are eligible. Despite this, we understand that the wireless industry is unbending in enforcing their current robotext policies, practices and processes by mandating all Medicaid agencies must satisfactorily demonstrate they receive prior express consent from enrollees to contact them before engaging in re-enrollment messaging campaigns—a position that is inconsistent with the public interest and the Bureau’s intent in the *Declaratory Ruling*.

Our members have also taken issue with certain aspects of wireless carriers’ use of existing methods of blocking behaviors which can degrade our members’ products. We again urge the Commission to conduct additional fact-finding and data collection on concerns related to the methods used by the wireless industry to contain illegal robotexting. In the end, it is consumers and our members’ customers that suffer. Appropriate fair and competitively neutral interoperability that is overseen by the Commission is necessary to promote public benefits for all end users and those service providers that seek to meet their demands, even while wireless network devices are clearly the predominant tool for individuals to communicate in the modern PSTN marketplace.

Before considering the Commission’s proposals in the *Further Notice*, INCOMPAS generally remains concerned about blocking of legitimate non-wireless 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. According to our members, the *Further Notice* overstates the extent to which service providers are providing notice when they block texts.<sup>5</sup> INCOMPAS urges the Commission to adopt a notification requirement in the event a text message is blocked by a downstream or terminating provider. While the *Order* took an encouraging first step in terms of requiring mobile wireless providers to maintain a single point of contact for texters to report erroneously blocked texts, the *Order* did not include a concomitant requirement to provide notice to an originating provider when a text message has been blocked. The Commission should act quickly to adopt a method to achieve immediate text blocking notification, such as the standardized use of a SIP Code or similar notification process. Without such a method, consumers and providers will have less opportunity to seek redress for blocked messages.

**Block Texts Upon Commission Notification:** With respect to the Commission's proposal 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, INCOMPAS understands the Commission's interest in extending the rule to text messaging, particularly given its recent decision to require gateway providers to block illegal robocall campaigns following agency notification. However, our members continue to believe that the ability to investigate and mitigate threats on their network is preferable to a more prescriptive blocking approach. If the Commission elects to adopt this proposal, INCOMPAS first recommends that the Commission ensure in its process that the method by which carriers identify and report suspicious behavior to the Commission must be competitively neutral. Before requiring providers to block text traffic, the Commission must issue a finding that the

---

<sup>5</sup> See *FNPRM* at para. 32.

traffic is illegal, with the Enforcement Bureau most likely relying on reports from wireless carriers operating under the current unregulated text messaging framework to make this finding. Without competitive neutrality in place—which would require the carriers to self-report their own bad actor customers and to use the same evaluation criteria whether the source of the traffic was their own customer or the customer of a third party—the Commission cannot offer assurances that the process is conducted in good faith and without anticompetitive concerns.

**Text Message Authentication and Spoofing:** The Commission seeks comment on how to encourage industry members to collaborate and finalize technical solutions for authenticating text messages and mitigating illegal text messages. INCOMPAS maintains that a caller ID authentication solution for text messaging could be valuable, but that the Commission should not mandate a technological solution for applying such authentication to robotexts until a standard is finalized and released. If the record 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 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. Given the progress that standards making bodies are making, it appears that text authentication and identification without discriminatory and unduly burdensome costs and process is achievable, but INCOMPAS implores the Commission to play an active role in the interoperability framework.

**Clarifying Do-Not-Call Protections for Text Messages:** The *Further Notice* also proposes to clarify and codify that National Do-Not-Call (“DNC”) protections apply to text messages as well as voice calls. INCOMPAS members have expressed concern that this

clarification is likely to lead to more erroneous blocking and subjective blocking policies with uneven enforcement given that the current unregulated text messaging framework does not have independent oversight or traceback procedures for purported DNC violations. Furthermore, our members suggest that consumers should be allowed to choose whether to apply these protections specifically to their text messages given that the Commission has allowed the messaging ecosystem to operate independently from the regulated voice service ecosystem for so long. Messaging consumers could be notified by the Commission that their DNC registrations will apply to text messages too and then be afforded a mechanism that would allow them to make an individual determination. Finally, INCOMPAS is concerned that this clarification could undermine basic security protections because much like the Medicaid scenario, non-wireless third-party, two-factor authentication providers could be prohibited from contacting end-users whose numbers are on the DNC, or could risk liabilities if improperly reported as calling/texting in derogation of the DNC rules.

**Closing the Lead Generator Loophole:** Finally, the Commission seeks to “ban the practice of obtaining a single consumer consent as ground for delivering calls and text messages from multiple marketers on subjects beyond the scope of the original consent” by amending the agency’s TCPA consent requirements such that “consent be considered granted only to callers logically and topically associated with the website that solicits consent and whose names are clearly disclosed on the same web page.”<sup>6</sup> With respect to the extent of the problem, many of our members indicate that they often do not allow lead generation contacts as part of their standard direct connect carrier contracts, despite the continued potential for perfectly legitimate

---

<sup>6</sup> See *FNRPM* at paras. 58, 61.

use cases for lead generation (i.e. civic engagement, insurance, health care, promotional channels, etc.).

As the Commission considers whether to close this loophole, some INCOMPAS members emphasize that it is extremely difficult for downstream providers to accurately verify that these text messages necessarily comply with the TCPA. While INCOMPAS members regularly verify through Know Your Customer protocols with direct customers that TCPA safeguards have been put in place, it is often not possible for providers that are two or more hops away from the originator if a TCPA check has been implemented. INCOMPAS urges the Commission to emphasize that call originators are the focus of any such requirements and not suggest liabilities for downstream providers that support due diligence with their own customers, but may inadvertently have non-compliant lead generation traffic exchanged through their networks.

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

Respectfully submitted,

**INCOMPAS**

*/s/ Christopher L. Shipley*

Christopher L. Shipley  
Executive Director of Public Policy  
INCOMPAS  
1100 G Street NW, Suite 800  
Washington, D.C. 20005  
(202) 872-5746  
cshipley@incompas.org

May 8, 2023