Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20544

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

COMMENTS OF THE VOICE ON THE NET COALITION

The Voice on the Net Coalition ("VON") submits these comments in response to the Commission's Further Notice of Proposed Rulemaking which seeks to bolster its new rules designed to combat unlawful text messages.[1] VON supports the Commission's interest in combating unlawful robotexts and welcomes sensible rules that restore competitive neutrality to the Commission's and industry's combined efforts to combat fraud and spam in the text messaging ecosystem.

The entire industry is aligned with the Commission's desire to reduce—if not eliminate entirely—scam text messaging. Competitive service providers, including providers like VON members, that serve a wide range of businesses, from small mom-and-pops to large enterprises, have implemented a number of methods to ferret out bad actors and prevent scam texts from leaving their platforms. At the same time, however, current industry efforts have resulted in anti-competitive registration requirements, which have lead to a significant market distortion that preferences large mobile wireless carriers over other SMS platforms. VON encourages the

[1] *Targeting and Eliminating Unlawful Text Messages*, Report and Order and Further Notice of Proposed Rulemaking, FCC No. 23-21, CG Docket Nos. 21-402 & 02-278 (rel. Mar. 17, 2023) ("*Order*", "*Further Notice,*" or "*FNPRM*").

Commission to avoid codifying these market distortions and restore competitive and technology neutrality to the text messaging ecosystem.

BACKGROUND

As technology has evolved, so has the SMS and MMS ecosystem. Text messages are no longer simply sent and received to and from individuals or among groups of individuals using mobile phones. Small businesses, such as wedding planners and financial advisors, send texts to their individual clients from apps on their computers or phones. Schools send out mass texts to the parents of their students with up-to-date notifications about school operations and events. Doctors' offices text patients appointment reminders, and food delivery apps let customers know when their driver is on the way with dinner. Competitive, non-wireless messaging providers, like VON Coalition members, support these use cases and more.

Unfortunately, in recent years, scam texts have persisted and robotexts have proliferated.[2] Bad actors still obtain SIM cards, send out multiple individual phishing texts from a mobile phone, and then switch to the next SIM card once the original number is shut down.[3] Companies send out mass market robotexts to individuals who may not realize that they "opted in" to receive such texts.[4] Bad actors, and some less reputable providers, leverage messaging to spam or defraud consumers en masse.

---

[2] *See Targeting and Eliminating Unlawful Text Messages*, Notice of Proposed Rulemaking, FCC No. 22-72, CG Docket No. 21-402, ¶ 3 (rel. Sept. 27, 2022) ("*NPRM*").

[3] *See, e.g.*, FCC, Consumer Advisory Committee, *Report on the State of Text Messaging*, at 11 (Aug. 30, 2022); CTIA, *Messaging Security Best Practices*, at 7 (June 2022), https://api.ctia.org/wp-content/uploads/2022/06/Messaging-Security-Best-Practices-June-2022.pdf.

[4] *See, e.g.*, Comments of the Electronic Privacy Information Center, et al. at 4-5, CG Docket 21-402 (filed Nov. 10, 2022); Reply Comments of Public Knowledge at 5-6, CG Docket No. 21-402 (filed Nov. 25, 2022).

Left to regulate itself, the industry has implemented useful solutions, such as text blocking and filtering before traffic leaves a provider's platform and the ability for customers to flag and report fraudulent or junk texts. The largest industry players have also implemented registration requirements for non-wireless customers that provide important diligence on marketing and other mass-messaging campaigns. Unfortunately, however, these registration requirements have also negatively impacted the use of conversational messaging by individual users on non-wireless messaging services.

VON supports the Commission's efforts to implement industry-wide rules to protect consumers. VON cautions the Commission to proceed deliberately and ensure that codified rules target the bad actors, are competitively and technology neutral, and do not allow existing market distortions to proliferate.

ARGUMENT

I. THE COMMISSION'S TEXT BLOCKING RULES MUST ENSURE TECHNOLOGICAL AND COMPETITIVE NEUTRALITY.

VON supports the Commission's efforts to require all messaging providers[5] to block suspected illegal traffic after receiving notice from the Enforcement Bureau,[6] but only if the Commission ensures illegal texting traffic is defined, reported, and addressed on a competitively and technologically neutral basis.

The FNPRM does not state how the Commission will identify suspected illegal messaging traffic or who will be responsible for reporting that traffic to the Commission. VON

---

[5] Although the FCC assumes that providers that offer SMS and MMS are "mobile wireless providers," *Order* ¶ 13 n.47, VON's members are among the many competitive non-mobile wireless providers that also offer SMS and MMS services interconnected with the mobile wireless networks. These competitive providers are a key piece of the legitimate SMS and MMS ecosystem.

[6] *FNPRM* ¶¶ 50-53.

cautions that any investigation into suspected illegal traffic must be applied evenly across the industry and blocking should only be required for confirmed—not merely suspected—illegal text traffic.

One option the Commission should consider adopting in conjunction with any text blocking mandates[7] is a traceback regime similar to the one used in the context of voice calling. For voice calls, the Industry Traceback Group ("ITG")—an independent, third-party group led by US Telecom and appointed by the Commission as the official US Traceback Consortium[8]—plays a key role. The ITG describes a suspected scam call and allows originating voice service providers to be notified, affording the originating providers with the opportunity to take action in the event that they had not already identified the activity themselves. Only in cases where the originating carrier does not take appropriate action is the Commission's intervention needed. Of importance, the ITG does not rely on providers to report their own customers and does not favor one segment of the industry over another.

Adding a traceback component to the Commission's text-blocking proposal would make this new obligation more competitively neutral and would avoid wasting Commission resources. A successful traceback-like mechanism would allow originating service providers to be notified about complaints from a Commission appointed third-party so that those service providers can take action on their own without having to burden Commission resources. The Commission should also establish criteria for determining what is a suspected illegal text message. Importantly, those criteria should be developed with input from the messaging industry as a

---

7 *FNPRM* ¶¶ 51-52.

8 *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, Report and Order, DA 22-870, EB Docket No. 20-22,, ¶ 1 (rel. Aug. 22, 2022).

whole (not just a subset of wireless carriers) and other interested stakeholders. And those criteria must be applied in a competitively neutral manner, regardless of whether the originator of suspected illegal traffic is a wireless carrier's own customer or is the customer of a third party.

VON also cautions the Commission against requiring blocking unless the Commission can confirm that the blocked traffic is illegal. Given that a blocking notice would come from a government agency (the Commission), requiring carriers to block this traffic on the basis of mere suspicion could implicate due process concerns as well as threaten First Amendment protections against prior restraint. These concerns underscore the need to ensure that a neutral third-party is responsible for both reporting traffic to the Enforcement Bureau and assisting with investigations.

II. ANY MESSAGING AUTHENTICATION AND REGISTRATION METHODS MUST ALSO BE TECHNOLOGICALLY AND COMPETITIVELY NEUTRAL.

As the Commission considers options for text authentication or registration, it must ensure that such requirements are competitively and technologically neutral. As VON noted in its comments on the NPRM in this proceeding, the primary industry solution intended to mitigate unlawful text messaging, registration with The Campaign Registry ("TCR"), has had significant anti-competitive effects.[9]

The TCR registration rules effectively impose registration requirements and fees on all non-wireless messaging providers of SMS and their customers, for all types of messaging traffic (both high-volume and conversational). These requirements can be very onerous and costly, and are applied even when message senders are engaged in conversational messaging between individuals. In contrast, TCR does *not* require registration or payment of related fees for

[9] *See* Comments of the Voice on the Net Coalition at 4-6, CG Docket No. 21-402 (filed Nov. 10, 2022).

wireless customers, even for business customers using messaging for business uses. One anticompetitive impact of this situation is that the native texting app on a mobile handset is treated as materially different from other messaging apps on the same mobile device offering the same capabilities. As the Commission has acknowledged, all forms of text messaging are subject to abuse,[10] and limiting authentication or registration (and payment) requirements to only certain types of providers or technologies ignores that reality. In addition, as explained above, the current TCR registration process is an inherently discriminatory arrangement that disadvantages non-wireless providers and their customers in both price and service quality. Any solution adopted by the Commission must not codify this existing regime.

VON strongly supports efforts to bring some form of authentication or registration obligation to high volume or mass market SMS messaging; it also supports requiring additional diligence to ensure good actors are following the rules in order to keep bad actors out of the ecosystem. If the Commission is inclined to adopt a mandatory registration or authentication regime, VON encourages the Commission to either designate a neutral third party to serve as the registration and/or authentication service or mandate that wireless carriers must accept traffic that has been registered and/or authenticated with a registration entity other than TCR. Any refusal by a mobile operator to accept traffic directly from another registration source should be reviewable by the Commission. This would help restore competitive neutrality and ensure that all messaging customers are protected from bad actors regardless of the technology used.

---

[10] *See NPRM* ¶ 6 (discussing abuse of person-to-person text messaging in the form of SIM card fraud); *see also Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al.*, Declaratory Ruling and Order, 30 FCC Rcd. 7961, 7970 ¶ 7 (2015) ("*TCPA of 1991 Decl. Ruling*") (stating that "[d]ialing options" are now "available via smartphone apps" that enable "[c]alling and texting consumers *en masse*").

III. THE COMMISSION SHOULD NOT IMPOSE STRICT LIABILITY ON PROVIDERS FOR CUSTOMERS' FAILURE TO COMPLY WITH NEW LEAD GENERATOR RULES.

The Commission rightfully notes that some bad actors are circumventing TCPA rules designed to protect consumers by obtaining "mass consent" from customers for messages that are not "logically and topically" related to the purpose for which the customer granted consent.[11] VON supports the Commission's efforts to hold entities liable for violating the TCPA and to better define what constitutes valid consent to receive marketing texts. This proposal tracks efforts that VON members are already taking. VON, however, urges the Commission to refrain from making service providers strictly liable for their customers' violations of any new rules.

Currently, VON members, like many others in the industry, undertake diligent efforts to "Know Our Customers" prior to offering service; require customers to contractually agree to comply with all laws, including the TCPA; monitor our networks to identify unusual or unexpected traffic patterns; and terminate customers who are violating the TCPA or other laws. Such reasonable efforts should be sufficient to shield providers from liability for bad actors' violations of any new requirements regarding consent.

Strict liability, on the other hand, is inconsistent with the *scienter* requirement that Congress and the courts have found has been required by the TCPA for decades[12] as well as with the Commission's requirement that, to be liable for violations of its TCPA rules, platforms must *knowingly* allow their customers to use the platform for unlawful purposes.[13] Strict liability

---

[11] *See FNPRM* ¶¶ 58-61.

[12] *See Warciak v. Subway Restaurants, Inc.*, 949 F.3d 354, 357 (7th Cir. 2020) ("In order to be held vicariously liable under the TCPA, an agent must have express or apparent authority.").

[13] *See, e.g.*, *TCPA of 1991 Decl. Ruling*, ¶ 30 ("Similarly, whether a person who offers a calling platform service for the use of others has *knowingly* allowed its client(s) to use that platform for unlawful purposes may also be a factor in determining whether the platform provider is so involved in placing the calls as to be deemed to have initiated them." (emphasis added)).

would also place service providers in an untenable position from a practical standpoint. It is nearly impossible for providers to determine which text messages are marketing messages versus, for example, transactional or personal messages, and then to verify whether all of their customers have requested and obtained legally valid opt-in consent from the recipients of all messages sent from those customers.

Requiring service providers to review the content of messages and to demand proof that consent has been obtained would require providers to review and regulate the speech of third parties as if that speech were their own. This proposal is a material departure from the balance expressed in the TCPA; moreover, a strict liability standard would exceed the Commission's authority to implement the TCPA without specific direction from Congress. Congress has made it clear that TCPA compliance obligations—including the obligation to comply with any new limitations aimed at lead generators—rest with the originator of the messages or calls, not the service provider.[14]

At most, the Commission should encourage service providers to continue requiring their customers—as a contractual matter—to comply with the Commission's rules by including those obligations in their terms of service and acceptable use policies while placing liability for TCPA violations on the originator of the messages or calls, as Congress intended.

[14] Ensuring that message service providers are not liable for the actions of their customers would also comport with the so-called "carrier exemption" in the TCPA, which excludes providers from liability for making any otherwise prohibited calls (including texts) "provided that the call is not charged to the called person or counted against the called person's plan limits on minutes or texts." 47 CFR 64.1200(a)(9).

CONCLUSION

VON looks forward to continuing to work with the Commission to prevent illegal text messages from reaching consumers. As we do so, it is important to ensure that new rules and mandates are competitively and technologically neutral and do not entrench existing market distortions that favor some providers over others.

Respectfully submitted,

Kristine Laudadio Devine
Julie Veach
HWG LLP
1919 M Street, NW, Suite 800
Washington, DC 20036
(202) 730-1338
kdevine@hwglaw.com
Counsel for the Voice on the Net Coalition

May 8, 2023