Testimony of
JAKE LESTOCK
CTIA

Oregon House Bill 3865

Before the House Commerce and Consumer Protection Committee

March 13, 2025

Chair Sosa, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I submit this testimony for the record regarding House Bill 3865. This bill would create new requirements to try to stifle illegal and unwanted robocalls by putting in place new restrictions on companies utilizing automated call technology and making violations of this legislation subject to the enforcement and penalties under Oregon's telephone solicitation and do not call laws.

CTIA and its member companies are committed to restoring trust in voice calls and maintaining trust in text messaging by working with federal and state policymakers and law enforcement agencies to stem the plague of illegal robocalls and text messages. This testimony describes the wireless industry's multi-layered and robust efforts to protect consumers from scam and spam text messages, while also supporting the legitimate text messages that consumers want.

While we appreciate the intent of House Bill 3865 to further protect Oregonians from unwanted calls or text messages, there are a few issues with this legislation as currently written that could have unintended consequences on Oregon businesses. We look forward to working with the bill sponsor and the committee to ensure that this legislation properly protects Oregon consumers from bad actors without creating uncertainty and harm to legitimate, law-abiding businesses.

Text Messages Remains Trusted Among Consumers and Non-Consumers

Wireless text messaging remains one of Americans' most popular and trusted forms of communication, and the wireless industry is dedicated to keeping it that way. Last year, Americans and exchanged more than 2.1 trillion text messages.[1] To continue this growth, wireless providers are constantly evolving their practices to support innovative uses of the platform while fighting spam and scam texts, including by blocking billions of spam text messages from ever reaching consumers. As just one metric, CTIA estimates that in 2023 wireless providers prevented over 47.5 billion spam messages from reaching consumers. The volume of blocked text messages has gone up as consumers increasingly use and trust the texting platform and bad actors turn their attention toward text messaging.

The Wireless Industry Is Working Hard to Maintain Consumer Trust in Text Messages

The Federal Communications Commission, wireless providers, and consumer advocates, have all recognized the broad scope of anti-scam efforts across the messaging ecosystem, including practices like up-front registration and vetting, monitoring, spam filters,

[1] CTIA, 2024 Annual Survey Highlights (Sept. 10, 2024), https://www.ctia.org/news/2024-annual-survey-highlights.

blocking algorithms, fraud investigation teams, and consumer reporting services, have gone a "long way to protect consumers."[2]

As a threshold protection against spam and scam text messages, wireless messaging technologies require valid originating information, such as a legitimate telephone number. As a result, number spoofing has not been the major issue in text messaging that it is in voice calling. Instead, impersonation scams – where bad actors use their own phone numbers but attempt to trick consumers into thinking that a trusted entity–like their bank–is contacting them for legitimate reasons, have been more prevalent. To address this issue, wireless providers and their ecosystem partners require businesses and other message senders to disclose information about themselves and their campaigns before they can send high volumes of text messages. This process has helped to weed out and prevent many bad actors from blasting out mass spam text messages, while also helping ensure that legitimate, wanted messages get through.

CTIA complements these technical processes with industry-leading guidance for message senders. Stakeholders throughout the messaging ecosystem have adopted CTIA's

[2] FCC, *Second Robotext Order*, 38 FCC Rcd 12247, ¶ 15 (rel. Dec. 18, 2023), https://docs.fcc.gov/public/attachments/FCC-23-107A1.pdf; *see also*, Letter from the National Consumer Law Center et al., to Marlene Dortch, Secretary, FCC, CG Docket Nos. 21-402 & 02-278, at 2 (filed Mar. 6, 2024) ("We believe that texting currently remains a valuable and trusted method of communication in the United States, largely because of the best practices developed by CTIA and adopted by its members and their partners.").

Messaging Principles and Best Practices, which encourage all non-consumer message senders, like a business or other organizations, to obtain consumer consent before sending messages.[3] The *Messaging Principles and Best Practices* help to ensure that consumers only get the messages they want to receive and not those they don't. Further, CTIA's *Messaging Security Best Practices* ask stakeholders throughout the ecosystem to play a significant role in helping to protect consumers from spam and to address leading sources of unwanted messaging. Wireless providers' commercial agreements and policies support these guidelines to protect consumers from unwanted messages and maintain consumer trust.

In addition to these frontline processes and best practices, wireless providers' security and fraud prevention teams use innovative technologies, like spam filters, machine learning, and other spam mitigation tools to protect consumers through real-time analysis and other defense solutions. To further enhance these protections, wireless providers have established a common means for consumers to report unwanted text messages – 7726 (SPAM). Wireless providers track and aggregate the information that consumers report through this channel and, together with industry partners, use that data to further calibrate their spam filters and

[3] CTIA, *Messaging Principles and Best Practices*, at 10 § 5.1 (May 2023) ("Messaging Principles and Best Practices"), https://api.ctia.org/wp-content/uploads/2023/05/230523-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf ("Regardless of whether [the FCC's rules] apply and to maintain Consumer confidence in messaging services, Non-Consumer Message Senders are expected to: [o]btain a Consumer's consent to receive messages generally; [o]btain a Consumer's express *written* consent to specifically receive marketing messages; and [e]nsure that Consumers have the ability to revoke consent.").

blocking tools to keep pace with the constantly changing tactics of bad actors. Wireless providers have also partnered with leading mobile operating system providers, Apple and Google, to make it easier for consumers to "Report Junk" directly through the wireless messaging applications associated with iOS and Android devices.

Despite all of these tools and capabilities, bad actors continue to seek out ways to get spam and scam text messages through to consumers. To help stop these bad actors, CTIA recently launched the Secure Messaging Initiative (SMI), an industry-led program that brings together experts in the private and public sectors, including wireless providers and messaging aggregators, as well as enforcement partners from federal and state entities to facilitate information sharing that can quickly thwart spam activity and help enforcement agencies target bad actors.

The SMI includes a collaborative, multi-stakeholder clearinghouse that provides a venue for increased partnership within industry and with Federal and State government agencies charged with investigatory and enforcement functions. The SMI participants share suspected spam messaging and activity with the clearinghouse, and that information is used by industry to complement tools to protect consumers, and it may be shared with government agencies to take action against bad actors at the source. Participants of the SMI will also share best practices and other information that can be used to further refine spam mitigation efforts.

Finally, CTIA and its member companies are developing new resources to help protect consumers from scam text messages. The comprehensive approach to protecting and educating consumers, and working with enforcement to stop bad actors, is discussed in more detail at FightingSpam.ctia.org.

In closing, the wireless industry is working hard to maintain trust in text messaging by protecting consumers from bad actors and enabling legitimate non-consumer message senders to reach consumers that want to receive their text messages. CTIA and its member companies look forward to working with Chair Sosa and other sponsors of House Bill 3865 to ensure that this legislation adequately targets bad actors while also avoiding any unintended consequences.