

Before the
Federal Communications Commission
Washington, D.C. 20554

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

NOTICE OF PROPOSED RULEMAKING

Adopted: September 23, 2022

Released: September 27, 2022

Comment Date: [30 days after Federal Register publication]
Reply Date: [45 days after Federal Register publication]

By the Commission:

I. INTRODUCTION

1. Text messaging is one of Americans' most popular forms of communication.1
Unfortunately for many consumers, illegal texts are becoming a common occurrence, just as illegal
robocalls have been for years. Such texts can present the same problems as illegal calls, from being an
annoyance at best to being used as vehicles for fraud at worst. While some mobile wireless providers
take measures to protect their customers, illegal text messaging appears to be an increasing problem for
consumers.

2. In this Notice of Proposed Rulemaking (NPRM), we propose to require mobile wireless
providers to block illegal text messages, building on our ongoing work to stop illegal and unwanted
robocalls. Specifically, we propose to require mobile wireless providers to block texts, at the network
level, that purport to be from invalid, unallocated, or unused numbers, and numbers on a Do-Not-
Originate (DNO) list. We also seek comment on the extent to which spoofing is a problem with regard to
text messaging today and whether there are measures the Commission can take to encourage providers to
identify and block texts that appear to come from spoofed numbers.2 In addition, we seek comment on
applying caller ID authentication standards to text messaging.

II. BACKGROUND

A. Magnitude of Problem

3. Commission data demonstrate that consumers are receiving increasing numbers of illegal
and unwanted text messages. In 2020, the Commission received approximately 14,000 consumer
complaints about unwanted text messages, representing an almost 146 percent increase from the number

1 Petitions for Declaratory Ruling on Regulatory Status of Wireless Messaging Services, WT Docket No. 08-7,
Declaratory Ruling, 33 FCC Rcd 12075, 12075, para. 1 (2018) (Wireless Messaging Declaratory Ruling); Letter
from Matthew Gerst, Assistant Vice President, Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC
(Nov. 16, 2018) (filed in WT Docket No. 08-7) at 1-2.

2 See, e.g., Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59, Fourth Report
and Order, 35 FCC Rcd 15221, 15236, para. 42 (2020) (Calling Blocking Fourth Report and Order) (stating that
terminating voice service providers must have in place a process to reasonably determine that the particular call
pattern is highly likely to be illegal before blocking calls).

of complaints the year before.³ The Commission has received 15,300 consumer complaints about unwanted texts in 2021 and 8,500 such complaints through June 30, 2022.⁴ While these numbers are lower than the complaints the Commission receives about unwanted calls,⁵ when compared to the total number of text messages exchanged each year,⁶ the increase is evidence of an emerging problem. Other data suggest the same.⁷

4. Unwanted text messages present the same problems as unwanted calls—they invade consumer privacy, and are vehicles for consumer fraud and identity theft.⁸ Text message-based scams also present harms beyond those of calls. Texts can include links to well-designed phishing websites that appear identical to the website of a legitimate company and fool a victim into providing personal or financial information. Texted links can also load unwanted software, including malware that steals passwords and other credentials, onto a device.⁹ Scam texts, like scam calls, may involve illegal caller ID spoofing, i.e., falsifying the caller ID information that appears on the called party's phone with the intent to defraud, cause harm, or wrongfully obtain something of value.¹⁰ In 2020, scammers stole over \$86 million through spam texting fraud schemes.¹¹ The median amount stolen from consumers in such scams was \$800.¹²

³ The Commission received 10,400 robotexting consumer complaints in 2018; 5,700 in 2019; 14,000 in 2020; and 15,300 in 2021. See FCC, Consumer Advisory Committee, Report on the State of Text Messaging at 9 (2022) (CAC Report).

⁴ See FCC, Consumer Alert, *Scam Robotexts are a Rising Threat*, (July 28, 2022), <https://www.fcc.gov/robotext-scams-rise>.

⁵ Each year, the Commission receives about 200,000 consumer complaints about unwanted calls, by far the largest source of consumer complaints. For example, robocall blocking company YouMail reports 4.5 billion robocalls in August 2022. See YouMail Robocall Index, available at <https://robocallindex.com/>.

⁶ In 2020, 2.2 trillion text messages were exchanged, representing 66,000 text messages per second. Consumers submitted one complaint for every nearly 80 million texts received.

⁷ For example, RoboKiller reports 7.4 billion spam texts sent in March 2021, which is more than the number of total robocalls in that month. RoboKiller, *Robocall Record: 7.4 Billion Spam Texts Surpass Total Robocalls by More Than 1 Billion Messages in March 2021* (Apr. 6, 2021), <https://www.robokiller.com/blog/march-2021-robocall-robotext-trends/>. See also Letter from Representative Raja Krishnamoorthi, Chairman, Subcommittee on Economic and Consumer Policy, Committee on Oversight and Reform, to Acting Chairwoman Jessica Rosenworcel, FCC (Aug. 20, 2021) available at <https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2021-08-20.RK%20to%20Rosenworcel-FCC%20re%20Spam%20Texts%20Briefing.pdf> (Krishnamoorthi August 20 Letter).

⁸ For more information on how to avoid or report unwanted calls and texts, see FCC, *Consumer Guides, Stop Unwanted Robocalls and Texts*, <https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts> (last visited Sept. 8, 2021); FTC, *How to Recognize and Report Spam Text Messages*, <https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages> (last visited Sept. 8, 2021).

⁹ Forbes, *Weaponized SMS Attack Goes Viral: What Millions Of Phone Users Need To Know* <https://www.forbes.com/sites/daveywinder/2021/04/29/weaponized-sms-attack-goes-viral-what-millions-of-phone-users-need-to-know/?sh=556abec064ab> (last visited Sept. 20, 2021).

¹⁰ See [Krishnamoorthi August 20 Letter](#) at 2 (discussing spoofed spam texts in Illinois), see also *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, WC Docket No. 17-97, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706, 9707, para. 3 (2017) (*2017 Call Blocking Report and Order*) (discussing spoofing in the robocall context); 47 U.S.C. § 227(e).

¹¹ See [Krishnamoorthi August 20 Letter](#) at 1.

¹² *Id.*

5. As discussed in the CAC Report, bad actors use ever-changing and increasingly complex tactics to commit fraud against consumers over text messages.¹³ In recent years, text scammers have taken a particularly sinister turn, such as engaging in COVID-19-related texting scams.¹⁴ Such scams demonstrate the scammers' willingness and ability to exploit consumers' concerns and fears. The Federal Trade Commission (FTC) recently alerted consumers to scammers' use of text messaging and email to steal consumers' money and personal information by touting bogus COVID-19 vaccine surveys.¹⁵ The FTC has also alerted the public about unemployment and personally identifiable information (PII) texting scams.¹⁶ The Internal Revenue Service's (IRS's) Dirty Dozen scam list for 2021 urges consumers to look out for the red flags of a texting scam.¹⁷ The IRS has seen an increase in phishing schemes using emails, letters, texts, and links, with keywords such as "Corona Virus," "COVID-19," and "Stimulus."¹⁸ These schemes are blasted to large numbers of people in an effort to get their PII or financial account information.

6. As the CAC Report describes, bad actors employ various techniques, such as creating a "SIM box," a device that can be loaded with 100s of SIM cards, to send significant volumes of text messages through a wireless provider's network by falsely acting as individual wireless phones to avoid the provider's volumetric filters.¹⁹ Another technique used to spread text messages is snowshoe messaging, where messages are spread across a list of phone numbers or short codes to avoid volume limitations.²⁰ Also, "account takeovers" are a significant source of unwanted messaging traffic and can take place when a bad actor gains unauthorized access to a message sender's account with a cloud-based provider and sends unwanted messages.²¹

7. How consumers receive text messages can exacerbate the problem of such scams. On many devices, consumers can immediately see some or all of the message, potentially piquing their interest and enticing them to open it and respond or click on a link within; whereas calls from unknown callers are often ignored by consumers. Furthermore, the ubiquitous use of text messaging, and the visual and/or auditory alerts that accompany these quick ways to communicate, encourage consumers' receptiveness to text messages.²² Data indicates that consumers read nearly all texts they receive, and do so nearly immediately.²³ Indeed, industry data suggests that consumers open a far larger percentage of text messages than email and open such messages much more quickly.²⁴

¹³ CAC Report at 11-12.

¹⁴ FCC, *COVID-19 Text Scams*, <https://www.fcc.gov/covid-19-text-scams> (last visited Sept. 26, 2022).

¹⁵ FTC, *Ignore Bogus COVID Vaccine Survey*, <https://www.consumer.ftc.gov/blog/2021/03/ignore-bogus-covid-vaccine-survey> (Sept. 26, 2022).

¹⁶ See, e.g., Seena Gressin, FTC, *Phishing Scheme Targets Unemployment Insurance Benefits and PII* (Sept. 26, 2022), <https://www.ftc.gov/news-events/blogs/business-blog/2021/08/businesses-phishing-scheme-targets-unemployment-benefits-pii>. See also Andrew Rayo, FTC, *Did you get a text from your own number? That's a scam*, (Apr. 11, 2022), <https://consumer.ftc.gov/consumer-alerts/2022/04/did-you-get-text-your-own-number-thats-scams>.

¹⁷ IRS, *IRS Announces Dirty Dozen Tax Scams for 2021* (June 28, 2021), <https://www.irs.gov/newsroom/irs-announces-dirty-dozen-tax-scams-for-2021>. See also IRS, *Tax Scams/Consumer Alerts, Scams Targeting Taxpayers*, <https://www.irs.gov/newsroom/tax-scams-consumer-alerts> (last visited Sept. 26, 2022).

¹⁸ IRS, *IRS Warns Against COVID-19 Fraud; Other Financial Schemes*, (June 8, 2020), <https://www.irs.gov/newsroom/irs-warns-against-covid-19-fraud-other-financial-schemes>.

¹⁹ CAC Report at 11.

²⁰ *Id.*

²¹ *Id.*

²² *Wireless Messaging Declaratory Ruling*, 33 FCC Rcd at 12079-80, para 12 & n.41.

²³ *Id.*

B. Regulatory Background

8. *Telephone Consumer Protection Act (TCPA)*. The TCPA generally requires callers to get consumer consent before making certain calls to consumers using an “automatic telephone dialing system” (also known as an “autodialer”) or an artificial or prerecorded voice.²⁵ While text messages do not use an artificial or prerecorded voice, since 2003, the Commission has applied the consent requirement to text messages using an autodialer and “made to a telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other common carrier service, or any service for which the called party is charged.”²⁶ In a recent decision, the Supreme Court clarified that “a necessary feature of an autodialer under § 227(a)(1)(A) is the capacity to use a random or sequential number generator to either store or produce phone numbers to be called.”²⁷

9. In 2015, the Commission also clarified that Internet-to-phone text messages, which are sent to a carrier’s server then routed to a consumer’s phone, are also covered by the TCPA’s protections.²⁸ The Commission observed that, “[f]rom the recipient’s perspective, Internet-to-phone text messaging is functionally equivalent to phone-to-phone text messaging,” and that, “the potential harm is identical to consumers; unwanted text messages pose the same cost and annoyance to consumers, regardless of whether they originate from a phone or the Internet.”²⁹ Accordingly, the Commission clarified that “consumer consent is required for text messages sent from text messaging apps that enable entities to send text messages to all or substantially all text-capable U.S. telephone numbers, including through the use of autodialer applications downloaded or otherwise installed on mobile phones.”³⁰

10. *National Do-Not-Call Registry (DNC)*. The DNC also protects consumers from unwanted text messages that contain marketing when the consumer has placed their number on the registry.³¹ DNC rules state that telemarketers, subject to certain exceptions,³² are prohibited from initiating any telephone solicitation to “[a] residential telephone subscriber who has registered his or her telephone number on the national do-not-call registry of persons who do not wish to receive telephone

(Continued from previous page)

²⁴ *Id.* at 12080, para. 12 & n.41.

²⁵ *See* 47 U.S.C. § 227(b)(1)(A).

²⁶ *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014, 14115, para. 165 (2003) (*2003 TCPA Order*). The Commission stated that this encompasses both voice calls and text calls to wireless numbers including, for example, SMS calls, provided the call is made to a telephone number assigned to such service. *Id.*

²⁷ *Facebook, Inc. v. Duguid*, 141 S.Ct.1163, 1171 (2021) (*Facebook*). The Court’s opinion may have narrowed the class of calling equipment callers consider to be autodialers and thus the number of text messages for which they seek consumer consent.

²⁸ *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, 30 FCC Rcd 7961, 8020, para. 114 (2015) (*2015 TCPA Declaratory Ruling and Order*).

²⁹ *Id.* at 8020, para. 115.

³⁰ *Id.* at 8020, para. 116.

³¹ *2003 TCPA Order*, 18 FCC Rcd at 14115-16, paras. 165-66. *See Emanuel (Manny) Hernandez, Click Cash Marketing, LLC, and Rock Solid Traffic*, Citation and Order Unauthorized Text Message Violations, 33 FCC Rcd 12382 (EB 2018) (*Hernandez Citation*) (Mr. Hernandez was responsive to the citation and no fine was issued.).

³² Exceptions include where the caller has prior express permission to call the consumer, or where the caller is calling on behalf of a tax-exempt nonprofit organization. *See 2003 TCPA Order*, 18 FCC Rcd at 14042-45, paras. 42-47; 47 CFR § 64.1200(f)(15)(i)-(iii) (exempting certain types of calls from the definition of “telephone solicitation”). There is also a safe harbor for telemarketers if they can demonstrate that any violation was the result of an error. *2003 TCPA Order*, 18 FCC Rcd at 14040, para. 38; 47 CFR § 64.1200(c)(2)(i)-(iii).

solicitations that is maintained by the Federal Government.”³³ The requirements apply to voice calls and text messages.³⁴

11. *Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM Act)*. The CAN-SPAM Act protects consumers from unwanted commercial email, including unwanted messages to wireless devices. Specifically, the CAN-SPAM Act and implementing rules cover all commercial email messages, which the law defines as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.”³⁵ This prohibition includes commercial text messages that originate as emails.³⁶

12. *Truth-in-Caller ID Act of 2009*. Just as with calls, illegal caller ID spoofing may be part of a scam text’s success.³⁷ The Truth In Caller ID Act of 2009 amended section 227 of the Act to prohibit caller ID spoofing³⁸ if the goal is to defraud, gain something of value, or otherwise cause harm.³⁹ The Commission updated its Truth in Caller ID rules in 2019 to encompass texts, as directed by the RAY BAUM’s Act.⁴⁰

13. *STIR/SHAKEN*. Caller ID authentication is an important tool to combat illegal caller ID spoofing, which allows voice service providers to verify that the caller ID information accompanying a call matches a number the caller is authorized to use. This in turn helps a voice service provider determine whether the call should be blocked or labeled.⁴¹ STIR/SHAKEN⁴² is a framework developed

³³ 47 CFR § 64.1200(c)(2); *2003 TCPA Order*, 18 FCC Rcd at 14034, para. 28.

³⁴ *2003 TCPA Order*, 18 FCC Rcd at 14115, para. 165. In 2003, the Commission revised the TCPA rules to establish the DNC in coordination with the FTC. *See id.* at 14034, para. 28. By revising the TCPA rules and establishing the DNC, the Commission provided consumers with options for avoiding unwanted telephone solicitations, including text messages.

³⁵ *See Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)*, 15 U.S.C. §§ 7701-7713. The implementing CAN-SPAM rules are at 16 CFR Part 316. For more information, *see* FTC, *CAN-SPAM Act: A Compliance Guide for Business*, <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business> (last visited Sept. 9, 2021).

³⁶ *Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, CG Docket Nos. 04-53, 02-278, Order, 19 FCC Rcd 15927, 15933-34, para. 16 (2004).

³⁷ *2017 Call Blocking Report and Order*, 32 FCC Rcd at 9707, para. 3.

³⁸ 47 U.S.C. § 227(e). Spoofing is when a caller deliberately falsifies the information transmitted to the caller ID display. The implementing rule is 47 CFR § 64.1604(a) (“No person or entity in the United States . . . shall, with the intent to defraud, cause harm, or wrongfully obtain anything of value, knowingly cause, directly or indirectly, any caller identification service to transmit or display misleading or inaccurate caller identification information in connection with any voice service or text messaging service.”). More information about spoofing can be found at FCC, Consumer Guide, *Caller ID Spoofing*, <https://www.fcc.gov/consumers/guides/spoofing-and-caller-id>. (last visited Sept. 9, 2021).

³⁹ 47 U.S.C. § 227(e); 47 CFR § 64.1604(a).

⁴⁰ *See Implementing Section 503 of the RAY BAUM’S Act*, WC Docket Nos 18-335, 11-39, Second Report and Order, 34 FCC Rcd 7303, 7306, para. 7 (2019). *See also* 47 CFR § 64.1600(o) (“Text message. The term ‘text message’: (1) Means a message consisting of text, images, sounds, or other information that is transmitted to or from a device that is identified as the receiving or transmitting device by means of a 10-digit telephone number or N11 service code; (2) Includes a short message service (SMS) message, and a multimedia message service (MMS) message . . .”).

⁴¹ STIR/SHAKEN allows providers to transmit calls with three levels of attestation. A voice service provider can indicate that: (i) it can confirm the identity of the subscriber making the call, and that the subscriber is using its associated telephone number (“A” or “full” attestation); (ii) it can confirm the identity of the subscriber but not the telephone number (“B” or “partial” attestation); or merely that (iii) it is the point of entry to the IP network for a call that originated elsewhere, such as a call that originated abroad or on a domestic network that is not STIR/SHAKEN-

(continued....)

for Internet Protocol (IP) networks to authenticate caller ID information and reduces the effectiveness of illegal spoofing.⁴³ STIR/SHAKEN standards, however, do not currently support text messages, although work on standards for text messages is underway.⁴⁴

14. *Enforcement.* In addition to the Commission’s regulatory policy, the Commission has enforced against illegal texting. For example, in December 2018, the Commission cited several entities for sending telemarketing text messages to numbers on the Do-Not-Call registry.⁴⁵

C. Call Blocking

15. While the Commission has taken significant steps to implement anti-robocalling rules, traditional enforcement remedies, standing alone, may not be sufficient deterrents. As a result, the Commission in recent years has taken steps to stop those calls before they reach consumers’ phones. The Commission has done so by permitting voice service providers to block unwanted and illegal phone calls, in addition to continuing to pursue enforcement actions against illegal robocallers.⁴⁶ These call blocking efforts do not apply to text messages.

16. Specifically, the Commission in 2017 authorized voice service providers to block, without consumer consent, certain categories of phone calls that are highly likely to be illegal, such as those purporting to be from invalid, unallocated, or unused numbers and numbers on a “Do-Not-Originate” (DNO) list.⁴⁷ In 2019, the Commission enabled voice service providers to block calls based on reasonable analytics designed to identify unwanted calls without consumers having to take any action, as long as consumers can opt out of the blocking service.⁴⁸ It further made clear that voice service providers could block all calls not on a consumer’s white list on an opt-in basis.⁴⁹

17. In the *Call Blocking Third Report and Order*, adopted in July 2020, the Commission enabled more voice service provider blocking by establishing two safe harbors from liability under the

(Continued from previous page) _____
enabled (“C” or “gateway” attestation). *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97, 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3245, para. 8 (2020) (*STIR/SHAKEN Order*).

⁴² SHAKEN, or Signature-based Handling of Asserted information using toKENS, and STIR, or Secure Telephony Identity Revisited, uses public key cryptography to provide assurances that certain information about the transmitted caller ID is accurate. *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876, 4883, para. 21 (2019) (*2019 Call Blocking Declaratory Ruling*).

⁴³ *Id.*

⁴⁴ See IETF, *Messaging Use Cases and Extensions for STIR*, Draft, at 2-3 (2021), <https://datatracker.ietf.org/doc/draft-ietf-stir-messaging/> (IETF Draft Standard).

⁴⁵ See, e.g., *Hernandez Citation*, 33 FCC Rcd 12382.

⁴⁶ In addition to our call blocking efforts, the rules we adopted to implement STIR/SHAKEN include measures that require intermediate and terminating voice service providers to accept only calls from providers with certifications in the Robocall Mitigation Database, which may result in fewer call from bad actors reaching consumers. See 47 CFR § 63.6305(c).

⁴⁷ *2017 Call Blocking Report and Order*, 32 FCC Rcd 9706, 9710-21, paras. 10-40. The *2017 Call Blocking Report and Order* specifically declined to apply these rules to text messages. *Id.* at 9706, para. 1 n.1.

⁴⁸ *2019 Call Blocking Declaratory Ruling*, 34 FCC Rcd at 4884-90, paras. 26-42.

⁴⁹ *Id.* at 4890-91, paras. 43-46.

Communications Act and the Commission's rules for erroneous call blocking.⁵⁰ The Commission built further on its work in December 2020, allowing voice service providers to block calls at the network level, without consumer opt in or opt out, if that blocking is based on reasonable analytics that incorporate caller ID authentication information designed to identify calls and call patterns that are highly likely to be illegal.⁵¹ The *Call Blocking Fourth Report and Order* also required all voice service providers to take steps to stop illegal traffic on their networks and assist the Commission, law enforcement, and the Traceback Consortium⁵² in tracking down callers that make such calls.⁵³

III. DISCUSSION

18. We propose to protect consumers from the increasing numbers of illegal text messages by extending some of our consumer protections against illegal phone calls to text messages.

A. Mandatory Blocking of Illegal Texts

19. *Mandatory Blocking of Texts Purporting to be From Invalid, Unallocated, or Unused Numbers or on the Do-Not-Originate List.* Similar to our approach to call blocking, we propose to require mobile wireless providers to block text messages at the network level (i.e., without consumer opt in or opt out) that purport to be from invalid, unallocated, or unused numbers, and numbers on the DNO list. These texts are highly likely to be illegal.⁵⁴ We seek comment on this proposal, including whether these text messages represent a material fraction of unwanted text messages. We seek comment on whether providers are blocking these types of messages today and, if so, how that blocking may inform our proposal. We seek comment on additional types of text blocking providers are currently doing, (e.g., blocking based on reasonable analytics). We seek comment on whether requiring mobile providers to block text messages at the network level is necessary or whether the Commission should simply continue to allow for such network level blocking. We also seek comment on whether numbers placed on the DNO list are used for illegal texts.

⁵⁰ *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, 7623-31, paras. 20-45 (2020) (*Call Blocking Third Report and Order*).

⁵¹ *Calling Blocking Fourth Report and Order*, 35 FCC Rcd at 15236, para. 42.

⁵² The Traceback Consortium is a group of voice service providers, wireline, wireless, and VoIP, that are tracing and identifying the source of illegal robocalls. For the latest Industry Traceback Report, see Industry Traceback Group, *Combating Illegal Robocalls*, <https://www.ustelecom.org/research/combating-illegal-robocalls/> (last visited Sept. 26, 2022). See also *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3113 (2020) (adopting rules for a registration process for a consortium to conduct private-led traceback initiatives); *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, Report and Order, 35 FCC Rcd 7886 (EB 2020) (selecting USTelecom's Industry Traceback Group as the consortium to conduct private-led traceback efforts).

⁵³ *Calling Blocking Fourth Report and Order*, 35 FCC Rcd at 15226-27, para 13.

⁵⁴ In the *2017 Call Blocking Report and Order*, in the context of blocking calls highly likely to be illegal, the Commission explained that phone numbers that are only used by their subscribers to receive inbound calls can be placed on a DNO list. These subscribers are generally government and enterprise users with call centers that receive calls on a specific toll-free number that is not used to make outbound calls; when the subscriber's number is spoofed without the subscriber's consent, the calls purporting to be from that number are most likely illegal. See *2017 Call Blocking Report and Order*, 32 FCC Rcd at 9710, para. 10. Further, use of an unassigned number, including an invalid number, provides a strong indication that the calling party is spoofing the caller ID to potentially defraud and harm a voice service subscriber and such calls are therefore highly likely to be illegal. *Id.* at 9713, para. 18. Calls purporting to use unallocated numbers are similar to calls purporting to use invalid numbers in that no subscriber can actually originate a call from any of these numbers, and therefore are highly likely to be illegal. *Id.* at 9715, para. 23.

20. *Additional Measures to Prevent Illegal Texts from Reaching Consumers.* We believe that additional measures may be necessary to prevent other types of illegal texts from reaching consumers. A particularly noxious type of scamming in the voice call context entails “spoofing,” whereby the caller disguises its number and instead shows the number of a neighbor or reputable source in the caller ID field in order to trick the recipient into thinking the call is trustworthy.⁵⁵ As noted above, the Truth In Caller ID Act of 2009 amended section 227 of the Act to prohibit caller ID spoofing and the Commission updated its Truth in Caller ID rules in 2019 to encompass texts, as directed by the RAY BAUM’s Act. In February 2021, the Alliance for Telecommunications Industry Solutions (ATIS), an industry standards group, stated this also occurs with text messages.⁵⁶ We seek comment on the extent to which spoofing is a problem with regards to text messaging.⁵⁷ We also seek comment on whether there are additional measures the Commission can take to encourage mobile wireless providers to block texts that appear to come from spoofed numbers.

21. *Need for Mandatory Blocking.* We seek comment on the need for mandatory blocking. Consumers can ignore a potentially unwanted or illegal phone call and have it sent directly to voice mail; text messages, however, can be harder to ignore and are more often opened immediately. We also believe that increases in illegal texts may be a result of our work to stop unwanted calls—incentivizing scammers and others to shift to texting. We seek comment on that belief and our view that we should bring text blocking more in line with call blocking by requiring blocking from invalid, unallocated, or unused numbers, and numbers that otherwise appear to be spoofed, and therefore reduce the incentive for scammers to migrate to texting.

22. How would our proposals affect any voluntary text blocking providers are doing now? We seek comment on the voluntary text blocking that providers are currently doing to protect their subscribers. How are providers protecting consumers in this regard today? What can we learn from voluntary text blocking efforts as we consider mandatory blocking?

23. We seek comment on the effectiveness of device-level or application-based text blocking to reduce illegal texts. We also seek comment on the prevalence of application-based (i.e., over the top, or OTT) text messaging and whether there are more or fewer illegal text messages sent on OTT services as opposed to through mobile wireless providers.⁵⁸ How do OTT messages differ in transmission characteristics from SMS and MMS texts, including their relationship to wireless telephone numbers? If OTT text messaging occupies the majority of the market, how likely are regulations such as those we propose, which are limited to mobile wireless providers, to mitigate the problem? We seek comment on whether the definition of “text message” in our current rules would apply to OTT messages sent to wireless telephone numbers, but not to OTT messages sent to other users within the same application.⁵⁹ We note that the current definition of text message, in the Truth in Caller ID rules, includes SMS messages but “does not include . . . a message sent over an IP-enabled messaging service to another user

⁵⁵ See *STIR/SHAKEN Order*, 35 FCC Rcd at 3242, para. 1.

⁵⁶ ATIS, *Robocalling and Communication ID Spoofing: Better Understanding Illicit and Unwanted Calls and How to Counter Them* at 25 (2021), https://access.atis.org/apps/group_public/download.php/57909/ATIS-I-0000081.pdf (ATIS Report).

⁵⁷ Compare ATIS Report at 25 (“with [text message] spam, it may be possible to analyze the contents of a message prior to delivery, enabling content-based mitigation techniques to be applied on a per-message basis”) with IETF, *Messaging Use Cases and Extensions for STIR*, Draft, at 2-3 (2021), <https://datatracker.ietf.org/doc/draft-ietf-stir-messaging/> (IETF Draft Standard) (“encrypted messaging is becoming more common, and analysis of message contents may no longer be a [reliable] way to mitigate messaging spam in the future”).

⁵⁸ OTT text messaging services use Wi-Fi or cellular data networks, whereas SMS/MMS uses the cellular network to send messages and photos.

⁵⁹ See 47 CFR § 64.1600(o).

of the same messaging service.”⁶⁰ We seek comment on the definition of text message to use in the text blocking context.

24. *Standards to Ensure Competitively- and Content-Neutral Grounds for Blocking.* We also propose that all tools that service providers use to determine whether a text is highly likely to be illegal be applied in a non-discriminatory, competitively- and content-neutral manner.⁶¹ For example, we propose that any blocking by a provider not be based solely or in part on the identity of other providers in the text’s transmission path. Nor may blocking be based on disfavored content. We thus seek comment on adopting the same “highly likely to be illegal” criteria that we have adopted for call blocking.⁶² We seek comment on additional standards for blocking that may prevent blocking of legal, legitimate (and wanted) texts, particularly in the case of one-to-many text messages.

25. *Emergency Texts.* We seek comment on whether and how to protect consumers from erroneous blocking of emergency text messages. Commission rules require Commercial Mobile Radio Service (CMRS) and certain other text messaging providers to send 911 text messages to Public Safety Answering Points (PSAPs) that are capable of receiving them.⁶³ Where the PSAP is not capable of receiving 911 texts, these providers must deliver an automatic bounce-back text message to any consumer attempting to text 911 stating that text-to-911 service is unavailable.⁶⁴ We believe it is improbable that text messages to 911 will be erroneously blocked under our rules. We nevertheless seek comment on the risk of erroneous blocking of texts to 911 and on any mechanisms or standards the Commission should adopt to mitigate such risks.

26. As a corollary, we seek comment on whether illegal texting to 911 poses a problem for PSAPs and, as a result, a threat to public safety. In addition, some text-capable PSAPs routinely send outbound text messages in response to hang-up calls or erroneously-dialed calls to 911. We seek comment on the risk of erroneous blocking of outbound texts from PSAPs and 911 call centers. Finally, are there other types of non-911 health and safety text communications, such as public health notices, text-based public safety alerts,⁶⁵ or texts to suicide prevention services such as the National Suicide Prevention Lifeline that are at risk of being erroneously blocked?⁶⁶ What mechanisms are available or should be developed to mitigate this risk?

27. *Mitigating Erroneous Blocking.* The Commission has acknowledged that call blocking comes with a risk that consumers could miss wanted calls, and we recognize the same concerns exist with our text blocking proposals. Because we only propose that text messages deemed highly likely to be illegal would be subject to blocking, we believe the risk of erroneous blocking to be minimal. We seek comment on this assumption. We seek comment on whether to apply safeguards to any text blocking requirements we might adopt.⁶⁷ For example, should we require that each terminating provider that

⁶⁰ 47 U.S.C. § 227(e)(8)(C).

⁶¹ The Commission stated that to be reasonable, analytics must be applied in a non-discriminatory, competitively neutral manner. *See 2019 Call Blocking Declaratory Ruling*, 34 FCC Rcd at 4888, para. 35.

⁶² *2017 Call Blocking Report and Order*, 32 FCC Rcd at 9710-21, paras. 10-40.

⁶³ *See* 47 CFR § 9.10(q)(10).

⁶⁴ *See* 47 CFR § 9.10(q)(3).

⁶⁵ Although the Wireless Emergency Alerts (WEA) system uses cell broadcasting rather than text messaging to send emergency alerts, many federal, state, and local authorities, as well as other emergency services providers, use text messaging as a complement to WEA to distribute emergency alerts and important safety information.

⁶⁶ *See Implementation of the National Suicide Hotline Improvement Act of 2018*, WC Docket No. 18-336, Second Report and Order, FCC 21-119 (rel. Nov. 19, 2021).. For general information about 988 and the National Suicide Prevention Lifeline, *see* FCC, *988 Suicide and Crisis Lifeline* (July 20, 2022) available at <https://www.fcc.gov/suicide-prevention-hotline>.

⁶⁷ 47 CFR § 64.1200(k)(8).

blocks texts provide a single point of contact, readily available on the terminating provider's public-facing website, for receiving text blocking error complaints and verifying the authenticity of the texts of a texting party that is adversely affected by information provided by caller ID authentication? If we do so, should we further require that the terminating provider must resolve disputes pertaining to caller ID authentication information within a reasonable time and, at a minimum, provide a status update within 24 hours? Further, when a texter makes a credible claim of erroneous blocking and the terminating provider determines that the texts should not have been blocked, or the text delivery decision is not appropriate, we seek comment on whether the terminating provider should be required to promptly cease the text treatment for that number unless circumstances change. We seek comment on this approach, and any alternative ways of addressing disputed or erroneous blocking. We also seek comment on whether we should adopt legal safe harbors for service providers as the Commission has done in the call blocking context.⁶⁸

B. Applying Caller ID Authentication Requirements to Text Messages

28. In order to facilitate blocking for certain types of illegal texts, we seek comment on whether to require providers to implement caller ID authentication for text messages.

29. Industry technologists developed caller ID authentication—specifically, the STIR/SHAKEN framework for IP networks—to combat spoofing of voice calls.⁶⁹ We seek comment on the progress of efforts to extend authentication to text messages. A working group of the Internet Engineering Task Force (IETF) is currently considering a draft standard regarding application of some components of the STIR/SHAKEN framework to text messages.⁷⁰ What additional work needs to be done on the draft standard currently under consideration? How long might it take to complete such work? Beyond that document, what if any additional standards work is necessary before authentication for text messages is operational?

30. Would the current STIR/SHAKEN governance system be able to accommodate authentication for text messages, or would it need to be modified or a new governance system established?⁷¹ Once standards work is sufficiently complete, what steps must providers take to implement authentication for text messages in their network? Can existing network upgrades to meet the June 30, 2021, STIR/SHAKEN implementation mandate for voice calls be used in whole or in part to support authentication for text messages? Or would authentication for text messages require more comprehensive technological network upgrades? If so, what is the estimated amount of time it would take to install the technology and what would be the projected costs?

31. We tentatively conclude that providers should implement caller ID authentication for text messages. We believe such a requirement would spur standards groups to complete development of standards promptly. Do commenters agree? What timeline should we establish for implementation that accounts for the time needed both to finish standards and for providers to perform any necessary network upgrades? Would two years be sufficient time to complete standards development and implement necessary technology? Should we instead require providers to implement caller ID for text messages when technically feasible, without setting a time-certain deadline? If so, how should we define “technically feasible”? Would this approach better account for uncertainty in the development process? Would it create a perverse incentive to delay development? Alternatively, is an implementation

⁶⁸ See 47 CFR § 64.1200(k)(11).

⁶⁹ See *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1862-65, paras. 5-12 (2020) (*Second Caller ID Authentication Report and Order*) (describing history and explaining technology).

⁷⁰ See IETF Draft Standard.

⁷¹ See *id.* at 3 (stating that “it seems likely that the governance structures put in place for securing telephone network resources with STIR could be repurposed to help secure the messaging ecosystem”).

requirement premature at this stage of standards development? If so, should we instead require providers to work to develop text caller ID authentication standards, similar to the Commission’s approach to non-IP caller ID authentication?⁷² Would this alternative approach sufficiently incentivize completion of new standards and deliver the benefits of those standards to Americans?

32. When it adopted the STIR/SHAKEN mandate, the Commission determined the expected benefits of implementing STIR/SHAKEN would far exceed estimated costs.⁷³ How can we quantify the benefit of protecting American consumers from spoofed texts through an implementation mandate for authentication for text messages? Are there any other benefits such a requirement would offer—for example, could authentication for text messages protect against malicious conduct toward text-to-911 services?⁷⁴ What would be the costs of an implementation mandate? Will small mobile service providers face particular challenges in authenticating text messages? How might we accommodate or mitigate such challenges?

33. We seek comment on the scope of any implementation mandate for authentication for text messages we adopt. Could we apply the requirement to providers of “voice service” who are subject to the STIR/SHAKEN implementation mandate⁷⁵ that also provide text message services,⁷⁶ on the basis that entities that both provide text messaging service and voice services are capable of implementing STIR/SHAKEN? Or should we define a new class of providers subject to a mandate for authentication for text messages? How would we define that class? What is our legal authority to create such a class and to regulate the members of any proposed class? Should we instead follow the definition of “text messaging service” from the Truth in Caller ID Act and apply this obligation to providers of such service?⁷⁷ Does this definition—which includes SMS messages but “does not include . . . a message sent over an IP-enabled messaging service to another user of the same messaging service”⁷⁸—adequately capture the scope of services Americans understand as “text message service” and through which bad actors defraud Americans using illegal and illegally spoofed robotexts? Should we extend the scope of any implementation mandate to include some or all OTT applications delivered over IP-based mobile data networks?⁷⁹ Rather than apply a mandate on a generally-defined class of text message service providers,

⁷² See 47 CFR § 64.6303(b) (requiring voice service providers with non-IP network technology to “[m]aintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-internet Protocol caller identification authentication solution, or active testing such a solution”).

⁷³ *STIR/SHAKEN Order*, 35 FCC Rcd at 3262, para. 45.

⁷⁴ See IETF Draft Standard at 3 (suggesting that “providing an identity assurance could help to mitigate denial-of-service attacks, as well as ultimately helping to identify the source of emergency communications in general (including . . . swatting attacks”).

⁷⁵ The Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (Dec. 30, 2019) (TRACED Act) required voice service providers to “implement the STIR/SHAKEN authentication framework” in the portions of their networks using Internet Protocol (IP), and to “take reasonable measures to implement an effective call authentication framework” in the non-IP portions of their networks no later than June 30, 2021. TRACED Act, § 4(b)(1)(A), (B). See *STIR/SHAKEN Order*; 35 FCC Rcd at 3252-3260, paras. 24-41. .

⁷⁶ See 47 CFR § 64.6300(l) (defining “voice service”).

⁷⁷ See 47 U.S.C. § 227(e)(8)(D) (defining “text messaging service” as “a service that enables the transmission or receipt of a text message, including a service provided as part of or in connection with a voice service”); see also 47 U.S.C. § 227(e)(8)(C) (defining “text message”).

⁷⁸ 47 U.S.C. § 227(e)(8)(C).

⁷⁹ As we explained in the *Text-to-988 Further Notice of Proposed Rulemaking*, “there are a variety of widely available text messaging services and platforms with different technological capabilities, including SMS, MMS, and
(continued....)

are there any unique types of providers we should focus our efforts on in particular?⁸⁰ Should we include interconnected OTT text messaging service providers?⁸¹

34. Is there a reason to apply any requirements to intermediate text message providers or aggregators, as in the STIR/SHAKEN context for voice calls?⁸² If we do apply requirements to intermediate providers, should we apply the requirement to intermediate providers who are subject to our existing STIR/SHAKEN rules and support text messages,⁸³ or use a new definition? If we adopt a new definition for “intermediate text message provider,” what should that definition be?

35. Should we subject voice service providers and intermediate providers (or the equivalent groups we establish for purposes of a rule) to substantially the same obligations as under the STIR/SHAKEN rules?⁸⁴ Or should we create new obligations specific to the text message context? If so, what obligations should we create? We also seek comment on other implementation issues. For instance, should we allow for extensions of the deadline for certain providers or classes of providers, or types of text messages? If we do allow for extensions, should we simply grant the same categorical extensions as the Commission did for the STIR/SHAKEN implementation mandate,⁸⁵ or are there differences between text message service providers and voice service providers that require different categories of providers to

(Continued from previous page)

‘over the top’ (OTT) applications delivered over Internet protocol (IP)-based mobile data networks. *Implementation of the National Suicide Hotline Improvement Act of 2018*, WC Docket No. 18-336, Further Notice of Proposed Rulemaking, 36 FCC Rcd 7943, 7957, para. 28 (2021) We further explained that “SMS requires use of an underlying carrier’s SMS Center (SMSC) to send and receive messages from other users while [MMS]-based messaging makes use of the SMSC but also involves the use of different functional elements to enable transport of the message over IP networks . . . A third category, ‘over-the-top’ (OTT) applications, may be offered by [mobile] providers or third parties and allow consumers to send text messages using SMS, MMS or directly via IP over a data connection to dedicated messaging servers and gateways. These OTT services, which are often downloaded through mobile app stores, are increasingly popular with consumers and may be interconnected with the PSTN or not. *Id.* at para. 28 n.95 (internal quotations omitted) (citing *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment*, PS Docket Nos. 11-153 and 10-255, Second Report and Order and Third Further Notice of Proposed Rulemaking, 29 FCC Rcd 9846, 9860, para. 28 n.85 (2014)).

⁸⁰ See, e.g., *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Third Further Notice of Proposed Rulemaking, 36 FCC Rcd 8827 (2021) (proposing to shorten the existing STIR/SHAKEN implementation extension for those small voice service providers most likely to originate illegal robocalls); *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket 17-59, WC Docket 17-97, Further Notice of Proposed Rulemaking, FCC 21-105 (Oct. 1, 2021) (proposing additional obligations on gateway providers to protect Americans against illegal robocalls originating abroad).

⁸¹ OTT applications may be offered by CMRS providers or third parties and allow consumers “to send text messages using SMS, MMS or directly via IP over a data connection to dedicated messaging servers and gateways.” *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment*, PS Docket Nos. 11-153 and 10-255, Second Report and Order and Third Further Notice of Proposed Rulemaking, 29 FCC Rcd 9846, 9860, para. 28 n.85 (2014) (*Text-to-911 Second Report and Order*).

⁸² See 47 CFR § 64.6302; see also *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1922-30, para. 132-150.

⁸³ See 47 CFR § 64.6300(f) (defining “intermediate provider”).

⁸⁴ See 47 CFR §§ 64.6301 (obligations on voice service providers), 64.6302 (obligations on intermediate providers).

⁸⁵ 47 CFR § 64.6304(a)-(d) (categorical extensions for (1) small voice service providers, (2) voice service providers that cannot obtain the certificate necessary to participate in STIR/SHAKEN; (3) services subject to a pending discontinuance application; and (4) non-IP networks); see also *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1876-1895, paras. 36-69.

receive extensions? Alternatively, should we follow the “undue hardship” standard⁸⁶ or some other standard to evaluate requested extensions?

36. Second, should we require providers with non-IP network technology to work to develop a non-IP solution to enable the authentication for text messages on non-IP networks,⁸⁷ or is there a different approach we could take to address non-IP network technology?⁸⁸ Third, should we prohibit providers from imposing additional line-item charges for authentication for text messages?⁸⁹ Fourth, should we establish rules regarding the display on subscriber devices of any information produced by authentication for text messages, or continue to take a hands-off approach to display?⁹⁰

C. Other Actions

37. We seek comment on other actions we could take to address illegal text messages. First, how can consumer education help to address the problem? Are there ways we could encourage consumers to file complaints about illegal text messages in order to inform and potentially enhance enforcement efforts?

38. Are there ways the Commission can enhance its spam text message consumer education outreach and content? Are there roles advisory committees such as the Commission’s Consumer Advisory Committee and the North American Numbering Council (NANC) could play in further educating consumers? We seek comment on whether text messages are more likely to be trusted than a call; if so, are there practices consumers and companies can adopt to maintain trust in text messages and to ensure they remain an effective tool for communication? We seek comment on how the Commission can educate consumers with regard to these practices.

39. *Digital Equity and Inclusion.* Finally, the Commission, as part of its continuing effort to advance digital equity for all,⁹¹ including people of color, persons with disabilities, persons who live in rural or tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations⁹² and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission’s relevant legal authority.

⁸⁶ See *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1876, para. 39.

⁸⁷ See 47 CFR § 64.6303(b).

⁸⁸ See IETF Draft Standard at 6 (“there will surely be cases where legacy transmission of messages will not permit an accompanying PASSport”); see also *id.* at 7 (explaining “a variety of non-SIP protocols . . . are responsible for most of the messaging that is sent to and from telephone numbers today”).

⁸⁹ 47 CFR § 64.6307; *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1920-22, paras. 126-31.

⁹⁰ *STIR/SHAKEN Order*, 35 FCC Rcd at 3266-67, para. 54.

⁹¹ Section 1 of the Communications Act of 1934 as amended provides that the FCC “regulat[es] interstate and foreign commerce in communication by wire and radio so as to make [such service] available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex.” 47 U.S.C. § 151.

⁹² The term “equity” is used here consistent with Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. See Exec. Order No. 13985, 86 Fed. Reg. 7009, Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (January 20, 2021).

D. Legal Authority

40. We seek comment on our authority to adopt the measures described in this Notice. Do we have authority under section 251(e), which provides us “exclusive jurisdiction over those portions of the North American Numbering Plan that pertain to the United States?”⁹³ The Commission found authority to implement STIR/SHAKEN for voice service providers under section 251(e) in order to prevent the fraudulent exploitation of numbering resources.⁹⁴ Does that section grant us authority to mandate implementation of authentication for text messages as well, or does it not apply to text messages? Similarly, we have relied on section 251(e) to support call blocking.⁹⁵ We seek comment on whether that authority extends to text messages. Would exercise of our ancillary authority—which the Commission relied on in part to apply an obligation on providers of interconnected text messaging services when it adopted text-to-911 requirements⁹⁶—be necessary or appropriate to support the proposed implementation mandate? Is there another relevant statute under which we hold authority to mandate that providers implement authentication for text messages? For example, might the TRACED Act or the TCPA provide authority for our proposals? Should the Commission seek additional authority in law from Congress? For example, we note above that the *Facebook, Inc. v. Duguid* decision may impact the scope of texts subject to the TCPA. We seek comment on the effect of that decision.

41. We seek comment on our authority under the Truth in Caller ID Act. We believe that the Truth in Caller ID Act provides authority for any implementation mandate we adopt pertaining to spoofing. That Act makes unlawful the spoofing of caller ID information “in connection with any telecommunications service or IP-enabled voice service or text messaging service . . . with the intent to defraud, cause harm, or wrongfully obtain anything of value.”⁹⁷ The Act directed the Commission to adopt rules to implement that section.⁹⁸ The Commission found authority under this provision to mandate STIR/SHAKEN implementation, explaining that it was “necessary to enable voice service providers to help prevent these unlawful acts and to protect voice service subscribers from scammers and bad actors.”⁹⁹ We believe that same reasoning applies here, especially given Congress’s focus on text messages, and seek comment on that conclusion.

42. We seek comment on the scope of our authority under Title III of the Act to undertake the measures described above.¹⁰⁰ Several provisions of Title III provide the Commission authority to establish license conditions in the public interest. For example, section 301 provides the Commission

⁹³ 47 U.S.C. § 251(e).

⁹⁴ *STIR/SHAKEN Order*, 35 FCC Rcd at 3260-61, para. 42.

⁹⁵ *2017 Call Blocking Report and Order*, 32FCC Rcd at 9727, para. 62.

⁹⁶ *See Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment*, PS Docket Nos. 10-255 and 11-153, Report and Order, 28 FCC Rcd 7556, 7600, paras. 128-40 (2013) (finding that applying bounce-back rules to these providers is “reasonably ancillary to the Commission’s effective performance of its statutorily mandated responsibilities and thus ‘necessary in the execution of its functions’”). *See also* 47 CFR § 154(i) (“The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions.”).

⁹⁷ 47 U.S.C. § 227(e)(1) (emphasis added).

⁹⁸ 47 U.S.C. § 227(e)(3).

⁹⁹ *STIR/SHAKEN Order*, 35 FCC Rcd at 3262, para. 44.

¹⁰⁰ *See, e.g., Empowering Consumers to Avoid Bill Shock, Consumer Information and Disclosure*, CG Dockets 10-207, 09-158, Notice of Proposed Rulemaking, 25 FCC Rcd 14625, 14639, para. 27 (2010) (describing potential sources of Title III authority in connection with the Commission’s bill shock proceeding). *See also Cellco P’Ship v. FCC*, 700 F.3d 534, 541-43 (D.C. Cir. 2012) (regarding the Commission’s broad spectrum management authority under Title III).

with authority to regulate “radio communications” and “transmission of energy by radio.”¹⁰¹ Under section 303, the Commission has the authority to establish operational obligations for licensees that further the goals and requirements of the Act if the obligations are in the “public convenience, interest, or necessity” and not inconsistent with other provisions of law.¹⁰² Section 303 also authorizes the Commission, subject to what the “public interest, convenience, or necessity requires,” to “[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class.”¹⁰³ Section 307(a) likewise authorizes the issuance of licenses “if public convenience, interest, or necessity will be served thereby.”¹⁰⁴ Section 316 provides a similar test for new conditions on existing licenses, authorizing such modifications if “in the judgment of the Commission such action will promote the public interest, convenience, and necessity.”¹⁰⁵ Would any of these provisions, or other provisions in Title III, furnish the Commission with authority to adopt our text blocking proposals? What other authority-related issues should the Commission consider? Does the public interest benefit of combating illegally spoofed robocalls fall within our “comprehensive mandate” to manage spectrum “in the public interest”?¹⁰⁶

E. Cost Benefit Analysis

43. *Expected benefits.* We anticipate that the blocking of illegal texts would achieve an annual benefit floor of \$6.3 billion. RoboKiller estimates that “Americans are on track to receive more than 86 billion spam texts in 2021, a 55% increase from 2020.”¹⁰⁷ Assuming a nuisance harm of 5 cents per spam text,¹⁰⁸ we estimate total nuisance harm to be \$4.3 billion (i.e., 5 cents x 86 billion spam texts).

44. We estimate that an additional \$2 billion of harm occurs annually due to fraud. As stated in our *STIR/SHAKEN Order*, American citizens lose approximately \$10.5 billion annually in fraudulent robocall offers.¹⁰⁹ Assuming that the corresponding loss through fraudulent texts is only 20% of that amount, the fraud loss from texts is \$2 billion annually. We seek comment on these benefit estimates. We also seek comment on whether our underlying assumptions are reasonable, and if not, what might be a better estimate of consumer harm. For instance, we have estimated a nuisance harm of 5 cents per spam text. Is such an estimate reasonable? If not, is there a range of consumer harm we should assess?

45. We expect that the combined total of \$6.3 billion to be a very conservative benefit floor which greatly understates total annual benefits. One reason is that RoboKiller reports¹¹⁰ that total spam texts grew by at least 55% in one year alone, i.e., from 2020 to 2021. RoboKiller explains that, because carriers have been successfully blocking a large share of illegal robocalls, that illegal traffic increasingly

¹⁰¹ See 47 U.S.C. § 301.

¹⁰² See 47 U.S.C. § 303 (stating that if the “public convenience, interest, or necessity requires” the Commission shall “(r)...prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this [Act]”).

¹⁰³ 47 U.S.C. § 303(b).

¹⁰⁴ 47 U.S.C. § 307(a).

¹⁰⁵ 47 U.S.C. § 316(a).

¹⁰⁶ See *Cellco Partnership v. FCC*, 700 F.3d 534, 541 (D.C. Cir. 2012) (quotation marks omitted).

¹⁰⁷ This figure is based on the RoboKiller estimate that “Americans are on track to receive more than 86 billion spam texts in 2021, a 55% increase from 2020.” *Total Robocalls Decrease by 3% in the First Month of STIR/SHAKEN Release* (Aug 6, 2021), <https://www.prnewswire.com/news-releases/total-robocalls-decrease-by-3-in-the-first-month-of-stirshaken-release-301350380.html>.

¹⁰⁸ See *STIR/SHAKEN Order*, 35 FCC Rcd at 3263, para. 47, where, for eliminating illegal scam robocalls, we assumed a benefit of ten cents per call.

¹⁰⁹ See *id.* at 3263, para. 48.

¹¹⁰ See *id.* at 3263, para. 48.

is shifting to spam texts.

46. Another reason this benefit floor is understated is that it does not include nonquantifiable benefits from reducing the delays caused in responding to text-to-911 calls by spam text-to-911 calls. Nor does it include the expected reduction in network congestion costs imposed on text service providers. We seek comment on these estimates and on our underlying assumptions.

47. *Expected costs.* As the Commission concluded in the *STIR/SHAKEN Order* with respect to the long-term cost of blocking illegal robocalls, we anticipate that our text blocking requirement would result in an overall reduction of costs to text service providers due to this expected reduction in network congestion costs.¹¹¹ Although the Commission will not obtain any detailed cost data until comments are received, we tentatively conclude the \$6.3 billion annual benefit floor expected from such a blocking requirement would far exceed the costs imposed on text service providers. We seek comment on this tentative conclusion.

IV. PROCEDURAL MATTERS

48. *Initial Regulatory Flexibility Analysis.* As required by the Regulatory Flexibility Act of 1980, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules addressed in the *Notice of Proposed Rulemaking*. The IRFA is set forth in the Appendix. Written public comments are requested on the IRFA. Comments must be filed by the deadlines for comments on the *Notice of Proposed Rulemaking* indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this IRFA to the Chief Counsel for Advocacy of the SBA.¹¹²

49. *Paperwork Reduction Act.* This document does not propose new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. In addition, therefore, it does not propose any new or modified information collection burden for small business concerns with fewer than 25 employees, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. § 3506(c)(4).

50. *Ex Parte Presentations—Permit-But-Disclose.* The proceeding shall be treated as a “permit-but-disclose” proceeding in accordance with the Commission's *ex parte* rules.¹¹³ Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with section 1.1206(b) of the Commission's rules. In proceedings governed by section 1.49(f) of the Commission's rules or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations,

¹¹¹ *See id.* at 3264, para. 51.

¹¹² *See* 5 U.S.C. § 603(a).

¹¹³ 47 CFR §§ 1.1200 *et seq.*

and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.¹¹⁴

51. *Comment Filing Procedures.* Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). See *Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998). Electronic Filers: Comments may be filed electronically using the Internet by accessing ECFS: <https://www.fcc.gov/ecfs/>.

52. Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. See *FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy*, Public Notice, 35 FCC Rcd 2788 (OMD 2020), <https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy>. In the event that the Commission announces the lifting of COVID-19 restrictions, a filing window will be opened at the Commission's office located at 9050 Junction Drive, Annapolis, MD 20701.¹¹⁵

53. Pursuant to section 1.49 of the Commission's rules, 47 CFR § 1.49, parties to this proceeding must file any documents in this proceeding using the Commission's Electronic Comment Filing System (ECFS): <http://apps.fcc.gov/ecfs/>.

54. *People with Disabilities.* To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice).

55. *Availability of Documents.* Comments, reply comments, and *ex parte* submissions will be available via ECFS. Documents will be available electronically in ASCII, Microsoft Word, and/or Adobe Acrobat. When the FCC Headquarters reopens to the public, these documents will also be available for public inspection during regular business hours in the FCC Reference Center, Federal Communications Commission, 45 L Street NE, Washington, D.C. 20554.

56. *Contact Person.* For further information about the *Notice of Proposed Rulemaking*, contact Mika Savir, Mika.Savir@fcc.gov or (202) 418-0384, of the Consumer and Governmental Affairs Bureau, Consumer Policy Division.

V. ORDERING CLAUSES

57. Accordingly, **IT IS ORDERED**, pursuant to sections 4(i), 4(j), 227(e), 251(e), and 303 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 227(e), 251(e), 303, that this *Notice of Proposed Rulemaking* IS ADOPTED.

58. **IT IS FURTHER ORDERED** that, pursuant to applicable procedures set forth in sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments on the Notice of Proposed Rulemaking on or before 30 days after publication in the Federal Register, and reply comments on or before 45 days after publication in the Federal Register.

59. **IT IS FURTHER ORDERED** that the Commission's Consumer and Governmental Affairs Bureau, Reference information Center, SHALL SEND a copy of this *Notice of Proposed Rulemaking*, including the Initial Regulatory Flexibility Analysis (IRFA), to the Chief Counsel for Advocacy of the Small Business Administration.

¹¹⁴ 47 CFR § 1.49(f).

¹¹⁵ See *Amendment of the Commission's Rules of Practice and Procedure*, Order, 35 FCC Rcd 5450 (OMD 2020).

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),¹ the Commission prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities by the policies and rules proposed in the Notice of Proposed Rulemaking (*Notice*). Written comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadline for comments on this *Notice*. The Commission will send a copy of the *Notice*, including the IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).² In addition, the *Notice* and IRFA (or summaries thereof) will be published in the Federal Register.³

A. Need for, and Objectives of, the Proposed Rules

2. The *Notice* seeks comment on requiring mobile wireless providers to protect consumers from illegal text messages by blocking at the network level text messages that are highly likely to be illegal because they purport to be from invalid, unallocated, or unused numbers and numbers on a Do-Not-Originate (DNO) list.

B. Legal Basis

3. This action, including publication of proposed rules, is authorized under sections (4)(i) and (j), 159, and 303(r) of the Communications Act of 1934, as amended.⁴

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

4. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules and policies, if adopted.⁵ The RFA generally defines the term “small entity” as having the same meaning as the terms “small business,” “small organization,” and “small governmental jurisdiction.”⁶ In addition, the term “small business” has the same meaning as the term “small business concern” under the Small Business Act.⁷ A “small business concern” is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.⁸

5. **Small Businesses, Small Organizations, Small Governmental Jurisdictions.** Our actions, over time, may affect small entities that are not easily categorized at present. We therefore

¹ 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601-612 has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 847 (1996).

² 5 U.S.C. § 603(a).

³ *Id.*

⁴ 47 U.S.C. §§ 154(i) and (j), 159, and 303(r).

⁵ 5 U.S.C. § 603(b)(3).

⁶ 5 U.S.C. § 601(6).

⁷ 5 U.S.C. § 601(3) (incorporating by reference the definition of “small-business concern” in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies “unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register.”

⁸ 15 U.S.C. § 632.

describe here, at the outset, three broad groups of small entities that could be directly affected herein.⁹ First, while there are industry-specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the SBA's Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.¹⁰ These types of small businesses represent 99.9% of all businesses in the United States, which translates to 28.8 million businesses.¹¹

6. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."¹² Nationwide, as of August 2016, there were approximately 356,494 small organizations based on registration and tax data filed by nonprofits with the Internal Revenue Service (IRS).¹³

7. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."¹⁴ U.S. Census Bureau data from the 2012 Census of Governments¹⁵ indicate that there were 90,056 local governmental jurisdictions, consisting of general purpose governments and special purpose governments, in the United States.¹⁶ Of this number, there were 37, 132 General purpose governments (county,¹⁷ municipal, and town or township¹⁸) with

⁹ See 5 U.S.C. § 601(3)-(6).

¹⁰ See SBA, Office of Advocacy, "Frequently Asked Questions, Question 1 – What is a small business?" https://www.sba.gov/sites/default/files/advocacy/SB-FAQ-2016_WEB.pdf (June 2016).

¹¹ See SBA, Office of Advocacy, "Frequently Asked Questions, Question 2- How many small businesses are there in the U.S.?" https://www.sba.gov/sites/default/files/advocacy/SB-FAQ-2016_WEB.pdf (June 2016).

¹² 5 U.S.C. § 601(4).

¹³ Data from the Urban Institute, National Center for Charitable Statistics (NCCS) reporting on nonprofit organizations registered with the IRS was used to estimate the number of small organizations. Reports generated using the NCCS online database indicated that as of August 2016 there were 356,494 registered nonprofits with total revenues of less than \$100,000. Of this number, 326,897 entities filed tax returns with 65,113 registered nonprofits reporting total revenues of \$50,000 or less on the IRS Form 990-N for Small Exempt Organizations and 261,784 nonprofits reporting total revenues of \$100,000 or less on some other version of the IRS Form 990 within 24 months of the August 2016 data release date. See <http://nccs.urban.org/sites/all/nccs-archive/html/tablewiz/tw.php> where the report showing this data can be generated by selecting the following data fields: Report: "The Number and Finances of All Registered 501(c) Nonprofits"; Show: "Registered Nonprofits"; By: "Total Revenue Level (years 1995, Aug to 2016, Aug)"; and For: "2016, Aug" then selecting "Show Results."

¹⁴ 5 U.S.C. § 601(5).

¹⁵ See 13 U.S.C. § 161. The Census of Government is conducted every five (5) years compiling data for years ending with "2" and "7." See also Program Description Census of Government <https://factfinder.census.gov/faces/affhelp/jsf/pages/metadata.xhtml?lang=en&type=program&id=program.en.COG#>

¹⁶ See U.S. Census Bureau, 2012 Census of Governments, Local Governments by Type and State: 2012 - United States-States, <https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG02.US01>. Local governmental jurisdictions are classified in two categories - General purpose governments (county, municipal and town or township) and Special purpose governments (special districts and independent school districts).

¹⁷ See U.S. Census Bureau, 2012 Census of Governments, County Governments by Population-Size Group and State: 2012 - United States-States. <https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG06.US01>. There were 2,114 county governments with populations less than 50,000.

¹⁸ See U.S. Census Bureau, 2012 Census of Governments, Subcounty General-Purpose Governments by Population-Size Group and State: 2012 - United States – States. <https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG07.US01>. There were 18,811 municipal and 16,207 town and township governments with populations less than 50,000.

populations of less than 50,000, and 12,184 Special purpose governments (independent school districts¹⁹ and special districts²⁰) with populations of less than 50,000. The 2012 U.S. Census Bureau data for most types of governments in the local government category show that the majority of these governments have populations of less than 50,000.²¹ Based on this data we estimate that at least 49,316 local government jurisdictions fall in the category of “small governmental jurisdictions.”²² Governmental entities are, however, exempt from application fees.²³

8. **Wireless Telecommunications Carriers (except Satellite).** This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.²⁴ The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.²⁵ For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year.²⁶ Of this total, 955 firms had employment of 999 or fewer employees and 12 had employment of 1000 employees or more.²⁷ Thus, under this category and the associated size standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small entities.

9. **All Other Telecommunications.** “All Other Telecommunications” is defined as follows: “This U.S. industry is comprised of establishments that are primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of

¹⁹ See U.S. Census Bureau, 2012 Census of Governments, Elementary and Secondary School Systems by Enrollment-Size Group and State: 2012 - United States-States.

<https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG11.US01>. There were 12,184 independent school districts with enrollment populations less than 50,000.

²⁰ See U.S. Census Bureau, 2012 Census of Governments, Special District Governments by Function and State: 2012 - United States-States. <https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG09.US01>. The U.S. Census Bureau data did not provide a population breakout for special district governments.

²¹ See U.S. Census Bureau, 2012 Census of Governments, County Governments by Population-Size Group and State: 2012 - United States-States - <https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG06.US01>; Subcounty General-Purpose Governments by Population-Size Group and State: 2012 - United States-States - <https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG07.US01>; and Elementary and Secondary School Systems by Enrollment-Size Group and State: 2012 - United States-States. <https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG11.US01>. While U.S. Census Bureau data did not provide a population breakout for special district governments, if the population of less than 50,000 for this category of local government is consistent with the other types of local governments the majority of the 38, 266 special district governments have populations of less than 50,000.

²² *Id.*

²³ 47 U.S.C. § 158(d)(1)(A).

²⁴ U.S. Census Bureau, 2012 NAICS Definitions, “517210 Wireless Telecommunications Carriers (Except Satellite).” See <https://factfinder.census.gov/faces/affhelp/jsf/pages/metadata.xhtml?lang=en&type=ib&id=ib.en./ECN.NAICS2012.517210>.

²⁵ 13 CFR § 121.201, NAICS code 517210.

²⁶ U.S. Census Bureau, 2012 *Economic Census of the United States*, Table EC1251SSSZ5, Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012 NAICS Code 517210. https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517210.

²⁷ *Id.* Available census data does not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is for firms with “1000 employees or more.”

transmitting telecommunications to, and receiving telecommunications from, satellite systems. Establishments providing Internet services or Voice over Internet Protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.”²⁸ The SBA has developed a small business size standard for “All Other Telecommunications,” which consists of all such firms with gross annual receipts of \$32.5 million or less.²⁹ For this category, census data for 2012 show that there were 1,442 firms that operated for the entire year. Of these firms, a total of 1,400 had gross annual receipts of less than \$25 million.³⁰ Thus, a majority of “All Other Telecommunications” firms potentially affected by the proposals in the *Notice* can be considered small.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

10. This *Notice* does not propose any changes to the Commission’s current information collection, reporting, recordkeeping, or compliance requirements.

E. Steps Taken to Minimize Significant Economic Impact on Small Entities, and Significant Alternatives Considered

11. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its approach, which may include the following four alternatives, among others: (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities.³¹

12. The *Notice* seeks comment on requiring mobile wireless providers to block text messages that are highly likely to be illegal. The *Notice* does not propose any exemptions for small entities. As service providers may already block landline and wireless calls that are highly likely to be illegal, the Commission does not anticipate that blocking such text messages will be burdensome for service providers.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

13. None.

²⁸ <http://www.census.gov/cgi-bin/sssd/naics/naicsrch>.

²⁹ 13 CFR § 121.201; NAICs code 517919.

³⁰ http://factfinder.census.gov/faces/tableservices.jsf/pages/productview.xhtml?pid+ECN_2012_US_51SSSZ4&prodType=table.

³¹ 5 U.S.C. § 603(c)(1)–(c)(4).