Federal Communications Commission

Consumer Advisory Committee

Report on the State of Text Messaging

August 30, 2022

Contents

Executive Summary

On April 25, 2022, the Federal Communications Commission ("FCC" or "Commission") requested in a Charge Letter that its Consumer Advisory Committee ("CAC") examine the problem of illegal and unwanted text messages and submit its findings in a Report by August 31, 2022. Specifically, the FCC directed the CAC to report on 1) the scope of the illegal and unwanted text problem; 2) how illegal and unwanted texts harm consumers and what are the best methods for consumers to avoid and/or manage these texts; 3) how the Commission should consider educating consumers on how they can evade such harms; 4) whether and how illegal text messages pose a threat to emergency telephone numbers (e.g. PSAPs, hospitals, and other emergency institutions) and how the Commission can protect emergency call centers without negatively impacting legitimate emergency text messages; and 5) how the Commission should take into account accessibility concerns when developing solutions to combat unwanted text messages. The CAC formed a Text Blocking Working Group ("Working Group") to develop this report.

The Working Group considered presentations and reviewed publicly available data to consider how to address each of the questions in the Commission's Charge Letter. The Working Group received presentations that summarized the text messaging ecosystem, including stakeholders and spam mitigation efforts, the types of scam text messages that consumers receive, research related to the volume of unwanted calls and text messages, the impact of robocalls on hospitals, accessibility considerations, and industry efforts and best practices to protect consumers. The Working Group also reviewed data from a variety of sources that provided statistics on consumer complaints and other metrics.

The Working Group observes that the messaging ecosystem has grown and evolved significantly over the past few decades. Through the years, industry stakeholders have deployed a variety of tools, processes, and best practices that have helped to build and maintain consumer trust in text messaging. There are a variety of ecosystem stakeholders that support numerous legitimate and innovative use cases for messaging while also protecting consumers from unwanted messages.

The Working Group discusses the various spam prevention and mitigation tools available today. In particular, the Working Group considers the existing laws in effect today to protect consumers, including the TCPA, Truth in Caller ID Act, TRACED Act, and more. The Working Group also reviewed industry tactics used to prevent and mitigate illegal and spam messages, including CTIA's *Messaging Principles and Best Practices*, industry spam prevention tools, anti-spam solutions, and consumer mitigations.

The Working Group offers several considerations for the Commission, including encouraging broader adoption of industry best practices, such as CTIA's *Messaging Principles and Best Practices*. Additionally, the Working Group recommends that the Commission and its federal and state government partners, as well as other stakeholders, enhance efforts to educate consumers to ensure they know how to protect themselves against unwanted messages, including network and device-level message blocking tools, and how to report unwanted messages through 7726 (SPAM).

In addition, the Working Group considered the impact of illegal text messages on Public Safety Answering Points ("PSAPs"). The Working Group considered the extent to which lessons from the Hospital Robocall Protection Working Group are applicable for preventing illegal and unwanted text messages from interfering with the operation of emergency services such as text-to-911. The Working Group did not find information to suggest that this is a significant issue for PSAPs today.

Finally, the Working Group discussed accessibility considerations for the Commission. The Working Group encourages the Commission to conduct more education and targeted outreach to the disability community to help enhance awareness of tools like 7726 (SPAM). The Working Group also recommends that the Commission ensure that educational materials use consistent terminology, provided in multiple languages, and be accessible to people with disabilities.

I. Background

A. Mission Statement

The Text Blocking Working Group ("Working Group") aims to present information to help the Federal Communications Commission ("FCC" or "Commission") protect consumers and the messaging platform from unwanted and illegal messaging.

B. Commission Charge: Letter and Text Blocking Working Group

On April 25, 2022, the Commission requested that its Consumer Advisory Committee ("CAC") examine the problem of illegal and unwanted text messages and to submit the findings in a Report by August 31, 2022 ("Charge Letter"). The Charge Letter directed the Report to include data and other information describing:

(1) The extent of the illegal and unwanted text problem;

(2) How illegal and unwanted texts harm consumers and what are the best methods for consumers to avoid and/or manage these texts;

(3) How the Commission should consider educating consumers on how consumers can evade such harms;

(4) Whether and how illegal text messages pose a threat to emergency telephone numbers (e.g., PSAPs, hospitals, and other emergency institutions) and how the Commission can protect emergency call centers without negatively impacting legitimate emergency text messages; and

(5) How the Commission should take into account accessibility concerns when developing solutions to combat unwanted text messages.

In order to complete the tasks required by the Charge Letter, the CAC formed the Working Group comprised of members of the CAC that represent consumer advocates, industry, academia, and state and local governments.

1. Scope of Review

The Working Group focused on two forms of wireless messaging, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS"). The original wireless messaging service, SMS, enables users to send and receive short text messages, typically 160 characters or fewer, to or from mobile phones and can support a host of applications. Today, the content that can be sent by wireless messaging is not limited to mere text. In particular, MMS is an extension of the SMS protocol and can deliver a variety of media and enables users to send pictures, videos, and attachments over wireless messaging channels.

SMS and MMS can reach those users with 10-digit numbers from the North American Numbering Plan that are SMS and MMS enabled (generally those associated with mobile phones). They can also reach toll-free numbers that have been appropriately text-enabled. In addition, wireless providers developed Common Short Codes ("CSCs"), which are 5- to 6-digit codes typically used by enterprises for communicating with consumers at high volume. Short codes are administered by the Common Short Code Administration, which leases the codes to applicants.[1]

The messaging ecosystem has also evolved to include a variety of wireless messaging services and providers. Facilities-based mobile wireless service providers that offer SMS and MMS generally provide them as native functions on a mobile device by using telephone numbers. But mobile service providers are not the only providers offering consumers the ability to send SMS and MMS. Applications providers (i.e., over-the-top ("OTT")) like WhatsApp and WeChat also offer wireless messaging service. Generally, these application providers offer wireless messaging service through apps that are downloaded from smartphone app stores. Some of these applications are used exclusively over the Internet and use Internet protocol ("IP") addresses for routing, and other applications also support sending and receiving SMS and MMS messages from mobile services providers, such as Apple's iMessage.

Others provide users with phone numbers that allow messages to be exchanged between telephone numbers and Internet endpoints. Consistent with the Charge Letter and Commission staff direction, these application-based messaging services were not examined by the Working Group.

Rich Communications Service ("RCS") is considered a successor technology to SMS/MMS and is an IP-based asynchronous messaging protocol. Real-time text ("RTT") are text communications that are transmitted over IP networks immediately as they are created (e.g., on a character-by-character basis), similar to voice calls. As RCS is a nascent service in the U.S. mobile wireless ecosystem, and RTT is specifically regulated by the FCC differently from SMS/MMS, RCS and RTT also were not examined by the Working Group.

2. Summary of Working Group Presentations

To develop the Report, the Working Group met generally on a weekly basis to receive presentations from experts in mitigating unwanted text messages, including wireless service providers and cloud-based providers, as well as consumer protection advocates. The Working Group received presentations that summarized the text messaging ecosystem, including stakeholders and spam mitigation efforts, the types of scam text messages that providers are mitigating, research related to the volume of unwanted calls and text messages, the impact of robocalls on hospitals, accessibility considerations, and industry efforts and best practices to protect consumers.

[1] Short codes are administered by the Common Short Code Administration (CSCA), an LLC governed by CTIA, the wireless trade association, on behalf of U.S. wireless carriers. Technical aspects of the registry are supported by CTIA's partner, iconectiv. *See* Short Code Registry, www.usshortcodes.com (last visited Aug. 17, 2022).

II. Consumers and Text Messaging

A. History and Growth of Text Messaging

Since its launch in 1992, text messaging has evolved into one of the most popular forms of communication for Americans, with trillions of wireless text messages sent each year in the U.S. In 2020, 2.2 trillion SMS and MMS messages were exchanged in America alone.[2] This averages to more than 6,750 SMS and MMS messages per American in 2020. Much of this increase was driven by the exchange of media, such as GIFs and videos over MMS.

American consumers, businesses, and many other entities are not only sending and receiving high volumes of text messages, but they are also actively engaging with them. SMS open rates are estimated to be as high as 98 percent and response rates as high as 45 percent.[3] These engagement rates eclipse email open and response rates – 20 percent and 6 percent, respectively. Further, consumers prefer texting over voice calling, nearly 2 to 1, and nearly half of all consumers text every single day (more than the use of any other communications medium, including voice or email).[4]

While not within the scope of this Report, the Working Group did consider how consumers use messaging apps to provide context for wireless messaging services. By 2015, the total global messaging volume of a single app, WhatsApp, was 50 percent larger than the messaging volume of the entire wireless provider-offered text messaging market.[5] Today, in the U.S., the volume of messages sent on application or OTT platforms is about five times the volume exchanged over SMS/MMS.

Given the availability, ease of use, and diverse capabilities, wireless text messaging has become one of the central tools of communications for many consumers. The Commission has previously noted that "[t]he tremendous growth of wireless messaging is attributable in large part to the fact that providers have been able to ensure the relatively spam-free nature of this service, which in turn has spurred a high degree of consumer loyalty to this method of communication, especially among younger Americans."[6] With the exponential and continuing growth in the

---

[2] CTIA, *2021 Annual Survey Highlights*, at 9 (July 27, 2021), https://api.ctia.org/wp-content/uploads/2021/07/2021-Annual-Survey-Highlights.pdf.

[3] Stanzie Cote, *The Future of Sales Follow-Ups: Text Messages*, Gartner (Oct. 4, 2019), https://www.gartner.com/en/digital-markets/insights/the-future-of-sales-follow-ups-text-messages; *see also, SMS Marketing Statistics 2022 for USA Businesses*, SMS Comparison USA (updated July 27, 2022) ("*SMS Marketing Statistics 2022*"), https://www.smscomparison.com/mass-text-messaging/2022-statistics/; *Email Marketing vs. SMS Marketing: You're Asking the Wrong Question* (Mar. 3, 2022), https://www.campaignmonitor.com/blog/emailmarketing/roi-showdown-sms-marketing-vs-email-marketing/. By contrast, email open rates are around 20 percent on average. *See SMS Marketing Statistics 2021*.

[4] Morning Consult Survey: Nationwide poll of 1,999 registered voters, conducted December 3-5, 2021.

[5] *See* Pal Karlsen & Pamela Clark-Dickson, *Mobile Messaging Traffic and Revenue Forecast: 2021-26*, Omdia (2021), https://omdia.tech.informa.com/OM019910/Mobile-Messaging-Traffic-and-Revenue-Forecast-2021-26 ; Tony Gunnarsson, *OTT Messaging Forecast Report: 2019-2024*, Omdia (2021).

[6] *Petitions for Declaratory Ruling on Regulatory Status of Wireless Messaging Service*, Declaratory Ruling, 33 FCC Rcd 12075, 12075 ¶ 1 (2018) ("*Declaratory Ruling*") (footnote omitted).

volume of wireless text messaging, the complaints about unwanted messages have increased, as described below.[7]

B. Consumer Trust in Text Messaging and Industry Efforts to Maintain It

As it stands today, consumers see messaging as one of the most trusted forms of communication compared to other popular alternatives such as email and voice calling. As noted above, messaging has a 98 precent open rate – significantly higher than email or other platforms. As the Commission has previously noted, wireless messaging is a trusted and reliable form of communication for many Americans.[8]

To maintain consumer trust and promote growth of the messaging platform, the wireless industry has established guidelines to encourage the innovative use of messaging by a variety of stakeholders, while also guarding against unwanted and unlawful text messages. For example, CTIA's *Messaging Principles and Best Practices* establish expectations that texts be sent only if consumers have provided consent to receive messages from businesses or other organizations, as well as the ability to revoke consent, acceptable content, and other provisions.[9] Stakeholders apply these guidelines to each other through commercial agreements and policies in conjunction with registration and vetting frameworks to protect consumers from unwanted messages and maintain consumer trust in the platform.[10] We note that CTIA's *Messaging Principles and Best Practices* are voluntary. It is still possible for senders of unwanted and illegal texts to send bulk texts without complying with these principles. The Working Group believes that greater adoption of CTIA's *Messaging Principles and Best Practices* would encourage more stakeholders to take steps to minimize unwanted messages.

As described below, messaging stakeholders use a variety of trained experts and automated tools to protect consumers and combat spam text messages while also protecting legitimate messages. Compared to the robocall context, where there is different data available to identify illegal and unwanted calls, innovative technologies in the messaging ecosystem apply sophisticated algorithms, which may include machine learning and artificial intelligence elements, to detailed data about text messages to enhance existing spam mitigation tools. Wireless providers' security and fraud prevention teams use these tools to protect consumers through real-time analysis and updating of rules-based protocols that are constantly evolving to help combat ever-changing

---

[7] National Consumer Law Center (NCLC), *Scam Robocalls: Telecom Providers Profit* (June 2022), https://www.nclc.org/images/pdf/robocalls/Rpt_Scam_Robocalls_May-2022.pdf.

[8] Declaratory Ruling, 33 FCC Rcd at 12080 ¶ 12.

[9] CTIA, *Messaging Principles and Best Practices*, at 12 (July 2019) ("*Messaging Principles and Best Practices*"), https://api.ctia.org/wp-content/uploads/2019/07/190719-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf.

[10] *See e.g.*, AT&T, *AT&T Code of Conduct for Short Code and 10-digit A2P SMS Messages* (Aug. 14, 2020), https://sinch.github.io/docs/sms/sms-other/downloads/ATT_Code_of_Conduct_062020.pdf; T-Mobile, *Code of Conduct* (Nov. 2020), https://www.t-mobile.com/support/public-files/attachments/T-Mobile%20Code-%20of%20Conduct.pdf; Twilio, *Twilio Messaging Policy* (Mar. 14, 2022), https://www.twilio.com/legal/messaging-policy; Aparna Khurjekar, *Let's keep text messaging services free of spam* (July 25, 2019) https://www.verizon.com/about/news/lets-keep-text-messaging-services-free-spam; *see also* 10DLC.org, Carrier Code of Conduct, https://www.10dlc.org/en/verizon-tmobile-att-sprint-carrier-code-of-conduct ("Verizon adopted a code of conduct based on the CTIA guidelines") (last visited Aug. 17, 2022).

tactics of bad actors. However, given the escalating number of complaints about unwanted and illegal texts, stakeholders will need to remain vigilant to respond to these changing threats.

The wireless industry's management of messaging services gives providers and other stakeholders many different tools and information sources to identify and mitigate unwanted messages. Industry shares this information with law enforcement, including the Federal Trade Commission ("FTC"), the Commission, and state Attorneys General, in an effort to collaboratively stop bad actors. In furtherance of these efforts, CTIA launched the Secure Messaging Initiative ("SMI") to help stop unwanted or illegal text messaging spam. The initiative includes a central clearinghouse that providers and government agencies can use to share suspected spam messages and techniques, as well as new *Messaging Security Best Practices* to provide guidance to stakeholders on how to address leading sources of unwanted messaging.[11]

C. Use Cases

There are several different ways text messaging can be used today. Text messages may be sent on a person-to-person basis from one consumer to another, the way friends, family, colleagues, and more use text messaging to communicate daily. Text messaging can also be used on an application-to-person basis, which covers all non-consumer to consumer messaging ("Non-Consumer"). Non-Consumer texting includes uses in which an entity (such as a business) uses an application to send messages to large numbers of end users.

Non-Consumer message senders may include, but are not limited to, large to small businesses, financial institutions, schools, medical practices, customer service entities, non-profit organizations, and political campaigns. Non-consumer messaging also includes mass-texting campaigns that send the same or similar messages to hundreds if not thousands of consumers with or without their prior express consent.[12]

Examples of how Non-Consumer messaging may be used include:[13]

- **Notifications** – Personalized alerts, reminders, and notifications for appointments, deliveries, and more.
- **Verifications** – One-time passwords for authentication to reduce fraud and protect consumers.
- **Promotions** – Marketing messages and offers to support sales or generate donations.

---

[11] Press Release, CTIA, *CTIA Announces Secure Messaging Initiative to Fight Spam Text Messages* (June 29, 2022), https://www.ctia.org/news/ctia-announces-secure-messaging-initiative-to-fight-spam-text-messages#:~:text=%E2%80%9CThe%20Secure%20Messaging%20Initiative%20builds,to%20help%20stop%20unwanted%20messaging.%E2%80%9D.

[12] *Declaratory Ruling*, 33 FCC Rcd at 12079 ¶ 10; *see also*, *Messaging Principles and Best Practices* at 8.

[13] Twilio, Use Cases, https://www.twilio.com/messaging/sms (last visited Aug. 17, 2022).

- **Conversational Care and Commerce** – Two-way communications between business or organizations to provide consumer support and engagement.

D. Overview of the Messaging Ecosystem

The messaging ecosystem has evolved to include a variety of wireless messaging services and providers.

1. Messaging Platforms and Services

There are multiple ways that text messages can be exchanged through the messaging ecosystem.

Text messages can be exchanged among consumers' mobile devices that are identified by 10-digit telephone numbers and routed through servers on mobile wireless networks using storage and retrieval functionality ("store and forward").[14] Non-Consumer messages can be originated by non-consumer message senders identified by a number of sources including 10-digit telephone numbers ("10DLC"), toll-free telephone numbers, or short codes, and delivered to a consumer's mobile device that is identified by a 10DLC.

Depending upon the identifier of the message senders (e.g., 10DLC, toll-free), each of these means of exchanging text messages is considered a distinct platform with differing purposes, use-cases, and applicable policies.[15] As described below, there are multiple entities that originate and route Non-Consumer text messages, including cloud-based providers, aggregators, and wireless service providers. Like consumer-to-consumer messages, Non-Consumer text messages are delivered to consumer mobile devices through servers on mobile wireless networks using "store and forward" functionality.

2. Ecosystem Stakeholders

There are several major types of entities that play different, key roles in the messaging ecosystem. Certain players may play multiple roles.

- **Non-Consumers** are the businesses, organizations, and other entities that originate messages to send to consumers.

- **Registrars** record a non-consumer's unique identifier, such as a 10-digit telephone number, verify associated information, evaluate the reputation of the message sender, including identity and messaging history, and confirm that senders have authority to use an identifier. In some cases, registrars also monitor non-consumer message senders to see whether they adhere to industry best practices or contractual agreements.

---

[14] *Declaratory Ruling*, 33 FCC Rcd at 12082-83 ¶ 19.

[15] *See* 10DLC.org, Home Page, https://www.10dlc.org/ (last visited Aug. 17, 2022); *see also*, CTIA, *Messaging Security Best Practices*, at 6 (June 2022) ("*Messaging Security Best Practices*"), https://api.ctia.org/wp-content/uploads/2022/06/Messaging-Security-Best-Practices-June-2022.pdf.

- **Cloud-Based Providers** enable non-consumers to send messages, among other communications services, through internet-based portals and applications over various channels to be delivered to consumers.
- **Aggregators** facilitate the flow of Non-Consumer messaging traffic from the cloud-based provider systems to each mobile wireless network.
- **Wireless Service Providers** validate that Non-Consumer messaging traffic is recorded by a registrar, monitor traffic to mitigate unwanted messages, and deliver messages to consumer mobile devices.

The following demonstrates the various roles of stakeholders in Non-Consumer messaging traffic:

- A **Non-Consumer** begins the flow of a text messages by registering an identifier (e.g., 10-digit telephone number) either directly with a **Registrar**, or indirectly through a **Cloud-Based Provider**. The cloud-based provider typically helps non-consumers with various aspects of their messaging campaigns, including obtaining identifiers to use to send their campaigns, and registering those identifiers with registrars, along with sending messages.
- The non-consumer will develop and input the text message into the cloud-based provider's system to originate the text message. The text message will be sent through the internet from the cloud-based provider to one or multiple **Aggregators**.
- An aggregator routes the text message through different mobile wireless networks operated by **Wireless Service Providers** who transform and process the text message so that it may be delivered to the consenting consumer's mobile wireless device.

III. The State of Illegal and Unwanted Text Messages and the Impact on Consumers

The Working Group reviewed data from the Commission, FTC, and industry experts to consider the scope and scale of illegal and unwanted text messages. In the past few years, complaints about unwanted text messages blocked by aggregators and wireless service providers have increased, as have the number of blocked illegal messages. The number of complaints about unwanted texts are a small fraction of the total number of texts sent.

A. Consumer Complaints (FCC, FTC)

Consumer complaints to the Commission and FTC can be informative of the volume of unwanted text messages. Complaints made in 2021 to the FCC about unwanted texts increased to 15,300 in 2021 from 5,700 in 2019.[16] Further, complaints to the FTC about unwanted texts increased to 377,840 in 2021 from 107,673 in 2019.[17] Given the volume of text messages

[16] FCC, Consumer Alert: Scam Robotexts Are Rising Threat (July 28, 2022), https://www.fcc.gov/robotext-scams-rise.

[17] FTC, *Consumer Sentinel Network*, Fraud Reports by Contact Method, Reports and Amounts by Contact Method (updated July 20, 2022), https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/LossesContactMethods (last

(trillions per year), this data suggests that consumers submitted one complaint for every nearly 80 million text messages.

The volume of complaints about text messages is still far lower than the volume of complaints about other platforms like robocalls. Indeed, the FCC has reported that the number of complaints about robotexts is only about one-third of the number of complaints about autodialed calls, and about one-quarter of complaints about spoofing violations in the voice context.[18]

B. Third-Party Data

Measuring SMS and MMS spam is a complex undertaking given the variety of data points, sources, and evolving tactics used by bad actors. Some third-party services provide information about the extent of unwanted text messages based on data available to them, with varying results. For example, Truecaller reported data that suggests there are more spam voice calls (robocalls) than spam texts – 31 spam calls per month compared to 19.5 spam texts[19] – while RoboKiller reports data that suggests there are more spam texts than robocalls. Other data may be available from other robocall blocking resources, such as YouMail[20] and Hiya.[21]

While useful to provide anecdotal or general trend data, the sources, methods, and extent of information available from third-party sources should be carefully evaluated before they are considered reliable sources of the actual number of unwanted calls or texts received. Data points that would inform this evaluation might include how many messages are reported as spam by consumers, how many messages consumers opt out of, and how many spam messages are blocked by providers. Other considerations include how the sources collect data, how they extrapolate from their sample to project larger trends, and how certain reports compare to other reports aimed at measuring similar subjects. Overall, measuring the scope and scale of illegal and unwanted text messages requires careful evaluation of all sources. Nevertheless, the growth in the number of complaints and the data provided by the third-party services indicates that the problem of unwanted texts is growing.

C. Sources of Illegal and Unwanted Text Messages

While the wireless industry has many tools to mitigate unwanted messages as described below, bad actors can slip through ecosystem spam prevention efforts. Bad actors may employ a variety of techniques to evade detection and get their spam messages through, potentially exploiting and harming consumers.

---

visited Aug. 18, 2022) (Losses & Contact Method tab, with quarters 1 through 4 checked for 2021 and 2020; indicating 644,048 fraud reports using the phone call contact method and 377,840 using the text contact method from Q1-Q4 2021, as compared with 382,036 phone call and 334,952 text fraud reports for Q1-Q4 2020).

[18] FCC, *Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information*, at 5 & 11 (Dec. 22, 2021).

[19] *Truecaller Insights 2022 U.S. Spam & Scam Report*, Truecaller Blog (May 24, 2022), https://truecaller.blog/2022/05/24/truecaller-insights-2022-us-spam-scam-report/.

[20] YouMail, Robocall Index, https://robocallindex.com/ (last visited Aug. 17, 2022).

[21] Hiya, State of the Call, https://www.hiya.com/state-of-the-call (last visited Aug. 17, 2022).

The Working Group heard presentations on the sources of illegal and unwanted messages from several industry stakeholders. In addition, the Working Group observes that CTIA's voluntary *Messaging Security Best Practices*[22] identify a number of activities that may threaten messaging security and propose steps stakeholders should take to protect against and address those threats.

While there appear to be many kinds of fraudulent campaigns, experts told the Working Group that there are likely only a few operators of these schemes – they just use different facades. Low barriers to access and use of subscriber identification module ("SIM") cards and telephone numbers are both resources that bad actors use to transmit unwanted text messages through industry spam prevention capabilities. Here are examples of how bad actors use these resources:

- **SIM cards** – Bad actors may create 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.

- **Snowshoeing** – Snowshoe Messaging is a technique used by bad actors to spread messages across a list of phone numbers or short codes to avoid volume limitations.[23] Snowshoe Messaging is closely tied to the use of disposable or temporary telephone numbers, which are low-cost or free telephone numbers that are generally obtained through a web-based service or prepaid SIM card purchases and are used for a temporary purpose.

Experts also told the Working Group that "account takeovers" are a significant source of unwanted messaging traffic. As an example, account takeovers may occur when, through social engineering, a bad actor gains unauthorized access to a Non-Consumer message sender's account with a cloud-based provider and sends unwanted messages. Social engineering may occur when bad actors specifically target someone with access to a Non-Consumer message sender's account by exploiting that person's trust to divulge account information or access malicious websites or attachments.[24] CTIA's *Messaging Security Best Practices* highlights steps that stakeholders should take to prevent account takeovers, such as implementing industry best practices to protect credentials and passwords and taking steps to shut down a compromised account.[25]

D. Tactics Used by Bad Actors to Defraud Consumers

Bad actors use ever-changing and increasingly complex tactics to commit fraud against consumers over text messages, including:

---

[22] *See generally Messaging Security Best Practices.*

[23] *Id*. at 7.

[24] Cisco, *What is Social Engineering?*, https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html (last visited Aug. 17, 2022).

[25] *Messaging Security Best Practices* at 7-8.

- **Phishing / SMShing** – Providing links to websites that direct consumers to provide personal information that can be exploited or sold to other bad actors or used to extract financial payments.

- **Imposter Fraud** – Impersonating legitimate businesses or government agencies to induce consumers to share personal information that can be exploited by bad actors or used to extract payments.

- **Emergency Scams** – Impersonating a family relative or friend on a claim that they are in need of financial assistance to extract payment from the consumer.

- **Gift or Inducements** – Offering fake gift cards or shopping sprees or other giveaways to induce consumers to disclose personal information that can be exploited to extract payments.

IV. Spam Prevention and Mitigation

The availability, ease of use, and high open rates make wireless messaging an ideal medium for all sorts of communications – including relaying urgent information to consumers (e.g., fraud alerts or flight changes). That popularity, however, also makes it attractive for bad actors, who may seek to employ a variety of techniques to exploit consumers and undermine trust in the messaging ecosystem. Enforcement of existing laws and implementation of industry best practices has helped to protect consumers and mitigate the transmittal of unwanted messages; however, the Commission and wireless service providers continue to receive a significant number of complaints about unwanted texts.

A. Enforcement of Laws and Rules

1. The TCPA

The Telephone Consumer Protection Act ("TCPA") and the Commission's implementing rules prohibit autodialed, prerecorded, or artificial voice calls or text messages to wireless telephone numbers without the prior express consent of the called party, unless the call is an emergency or one of a small number of other exceptions applies.[26] Text messages sent using any automatic telephone dialing system ("autodialer") are subject to the TCPA and FCC rules. To the extent that text messages are sent using an autodialer, the TCPA's restrictions do not apply if the text message sender obtains the recipient's prior express consent.[27] Consumers may revoke consent through "any reasonable means," including any manner that clearly expresses a desire not to receive further messages (e.g., STOP).[28]

[26] 47 C.F.R. § 64.1200(a).

[27] *See* 47 U.S.C. § 227(b)(1); 47 C.F.R. § 64.1200(a).

[28] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Declaratory Ruling and Order, 30 FCC Rcd 7961, 8014-22 ¶¶ 107-122 (2015).

A threshold question as to whether the TCPA applies is whether the equipment used to send text messages is an "autodialer." Over nearly 30 years, the FCC has provided guidance on how to determine whether equipment is an autodialer, while various courts have provided their own interpretations that have led to conflicting rulings. In 2021, the U.S. Supreme Court ruled on the issue of defining an "autodialer," and interpreted that term to apply to a narrow range of technologies.[29] As a result of this decision, the TCPA may now play a more limited role in protecting consumers because that decision had the effect of narrowing the scope of messaging traffic subject to the protections of the TCPA. The FCC's proceeding to re-evaluate the definition of "autodialer" remains open.

2. Truth in Caller ID Act

The Truth in Caller ID Act of 2009 prohibits anyone from causing a caller ID service to knowingly transmit misleading or inaccurate caller ID information ("spoofing") with the intent to defraud, cause harm, or wrongly obtain anything of value.[30] Congress expanded the Truth in Caller ID Act to encompass text messaging in the RAY BAUM's Act in 2018, and the FCC subsequently adopted implementing rules.[31] The FCC's rules apply to SMS and MMS using ten-digit telephone numbers, toll-free telephone numbers, and short codes. These rules allow the FCC to bring enforcement actions against bad actors who spoof telephone numbers to send text messages.

3. TRACED Act

In the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act of 2019 ("TRACED Act"), Congress directed the FCC to establish regulations to create a process that "streamlines the ways in which a private entity may voluntarily share with the Commission information relating to" a call or text message that violates prohibitions regarding the TCPA and Truth in Caller ID rules.[32]

Last year, the FCC adopted rules and directed the Enforcement Bureau to create an online portal for such information sharing.[33] The purpose of the portal is to enable private entities to voluntarily share information about suspected robocall and spoofing incidents. "Private entities" do not include consumers who may submit complaints about unwanted text messages through the FCC's complaint process.

---

[29] *Facebook, Inc. v. Duguid*, 141 S. Ct. 1163 (2021).

[30] *See* 47 U.S.C. § 227(e).

[31] Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, Div. P, Title V, § 503, 132 Stat. 348, 1091-94 (2018) (codified as amended in 47 U.S.C. § 227(e)); *Implementing Section 503 of RAY BAUM'S Act*, Second Report and Order, 34 FCC Rcd 7303 (2019); 47 C.F.R. § 64.1600, *et. seq.*; 47 C.F.R. § 64.1604.

[32] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, § 10(a), Pub. L. No. 116-105, 133 Stat. 3274 (2019) ("TRACED Act").

[33] *See Implementing Section 10(a) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, Report and Order, 36 FCC Rcd 10673 (2021); 47 C.F.R. § 64.1204; 47 C.F.R. § 64.1606.

Once launched, the portal will enable private entities to submit certain minimum information, including the name of the reporting entity, contact information, at least one individual name and means of contacting the entity (e.g., a phone number), the caller ID information displayed, the phone number(s) called, the date(s) and time(s) of the relevant calls or texts, the name of the reporting private entity's service provider, and a description of the problematic calls or texts.

The FCC's Enforcement Bureau may share information gathered from the portal with other government agencies combatting robocalls, including the Department of Justice, FTC, state attorney general offices, and other law enforcement entities with which the Commission has information sharing agreements, as well as industry partners.

4. Unfair and Deceptive Practices

Section 5(a) of the Federal Trade Commission Act states that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful."[34] The FTC enforces this prohibition.[35] In addition, every state has a law that prohibits unfair or deceptive practices, although these laws may vary by state.[36] The FTC has used its authority to take action against bad actors, as well as educate consumers about how to recognize and report unwanted text messages.[37]

5. CAN-SPAM Act

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act") and FCC rules prohibit commercial e-mail messages sent using internet-to-phone SMS services without prior express authorization of the addressee.[38] Internet-to-phone SMS services enable a sender to initiate or send e-mail messages to an internet domain associated with a wireless service (e.g., 2025551234@carrier.com). Phone-to-phone text messages are not covered by the CAN-SPAM Act. The FCC maintains a list of wireless internet domain names based on information that wireless providers are required update.[39] The FTC generally enforces the CAN-SPAM Act, but sector-specific agencies enforce it with regard to parties they regulate

---

[34] 15 U.S.C. § 45(a)(1).

[35] *Id*. § 45(b).

[36] *See* Carolyn L. Carter, *Consumer Protection in the States; A 50-State Report of Unfair and Deceptive Acts and Practices Statutes*, National Consumer Law Center Inc. (Feb. 2009), https://www.nclc.org/images/pdf/udap/report_50_states.pdf.

[37] *See, e.g.,* Andrew Rayo, *Did you get a text from your own number? That's a scam*, FTC (Apr. 11, 2022), https://consumer.ftc.gov/consumer-alerts/2022/04/did-you-get-text-your-own-number-thats-scam; Press Release, FTC, *FTC Cracks Down on Senders of Spam Text Messages Promoting "Free" Gift Cards* (Mar. 7, 2013), https://www.ftc.gov/news-events/news/press-releases/2013/03/ftc-cracks-down-senders-spam-text-messages-promoting-free-gift-cards.

[38] *See* 15 U.S.C. § 7701, *et. seq.*; 47 C.F.R. § 64.3100, *et. seq*.; 16 C.F.R. § 316, *et. seq.*

[39] FCC, Consumer Policy Division, CAN-SPAM, Domain Name Downloads, https://www.fcc.gov/consumer-governmental-affairs/about-bureau/consumer-policy-division/can-spam/domain-name-downloads# (last visited Aug. 17, 2022).

(e.g., the FCC enforces with regard to parties subject to the Communications Act), and states may take enforcement action in certain circumstances.

B. Industry Tactics Used to Prevent and Mitigate Illegal and Spam Messages

Collaboration, information sharing, and action among wireless messaging stakeholders and appropriate law enforcement agencies are necessary to minimize unwanted messages and protect consumers. Additionally, the following describes various tactics that stakeholders use to prevent and mitigate unwanted messages.

1. CTIA's Messaging Principles and Best Practices

Beyond rules enforced by the FCC (described above), the wireless ecosystem provides substantial protections for consumers and enhances consumer trust in the voice and messaging platforms, while at the same time supporting legitimate uses of those platforms, by adopting and implementing best practices. CTIA's *Messaging Principles and Best Practices* reflect industry practices that have evolved over two decades to protect consumers from unwanted texts and support a robust and dynamic ecosystem where wanted messages can be exchanged between enterprises and consumers. Wireless providers and other stakeholders have created their own commercial agreements, policies, and frameworks that implement these *Messaging Principles and Best Practices*.

CTIA's *Messaging Principles and Best Practices* identify the following core principles to protect consumers from illegal and unwanted messages:[40]

- "All Service Providers should use reasonable efforts to prevent Unwanted Messages from being sent by or to Consumers;
- All Service Providers may filter or block Unwanted Messages before they reach Consumers;
- To the extent practical and consistent with Service Providers' Unwanted Message prevention and mitigation methods, Service Providers may notify the Message Sender sending Unwanted Messages when Service Providers block Unwanted Messages;
- Service Providers should adopt Unwanted Messaging traffic practices that protect Consumers in a manner that facilitates the exchange of wanted wireless messaging traffic; and
- Where appropriate, wireless ecosystem members should collaborate to maintain Consumer trust and confidence in wireless messaging services."

A Message Sender's failure to abide by such principles may increase the risk that a Message Sender's messages are blocked.[41] The *Messaging Principles and Best Practices* have helped the

[40] *Messaging Principles and Best Practices* at 21; *id*. at 9 (defining "Service Providers" as any party that offers messaging services or messaging-related services to Consumers or Non-Consumers using 10-digit NANP telephone numbers or short codes, including Wireless Providers, MVNOs, Cloud-Based Providers, and CLECs).

[41] *Messaging Security Best Practices* at 6-7.

wireless industry consistently mitigate spam over text messaging and bolster trust. However, they are voluntary, and bad actors have sometimes been successful in evading industry best practices.

2. Industry Spam Prevention Tools

a. Registration, Vetting, and Know Your Customer

Collecting and maintaining accurate information about message senders form an important means of preventing and mitigating unwanted messages. With accurate information, stakeholders can prevent unwanted messages from being delivered to consumers, and can share information with each other and with law enforcement agencies to stop bad actors from further sending such messages.

As described above, registrars record a non-consumer's unique identifier, such as a 10-digit telephone number, verify associated information, evaluate the reputation of the message sender, including a message sender's identity and messaging history, and confirm that senders have authority to use an identifier. In some cases, registrars also monitor non-consumer message senders' adherence to industry best practices or contractual agreements.

To assist with potential forensic analysis efforts and identify a message sender sending unwanted messages, cloud-based providers and aggregators, among other stakeholders, are expected to undertake reasonable efforts to "know their customer" by obtaining sufficient identifying information to verify or authenticate a message sender's identity before the message sender sends a message.[42]

CTIA's *Messaging Security Best Practices* describes the type of information about message senders that can help stakeholders prevent and mitigate unwanted messages, including:[43]

- The message origination point (e.g., IP address, telephone number, or other information associated with the message sender);
- Message destination (e.g., IP address, telephone number, or other information associated with the recipient);
- The date and time of the message;
- Session Initiation Protocol (SIP) header anomalies;
- Evidence that the message was an unwanted message (e.g., evidence that the message was abusive, harmful, malicious, unlawful, or otherwise inappropriate); or
- The volume of messages.

[42] *Id.* at 5.

[43] *Id.* at 4-5.

By maintaining accurate information about message senders and sharing actionable information about bad actors, messaging ecosystem stakeholders can apply a variety of anti-spam solutions to minimize unwanted messages.

b. Anti-Spam Solutions

The Working Group heard about a variety of tools that messaging ecosystem stakeholders use to prevent unwanted messages from being delivered to consumers.

- **Spam Filters** –Wireless providers and their partners throughout the messaging ecosystem actively monitor daily text messaging traffic for factors like high throughput and volume, using innovative techniques like artificial intelligence and machine learning to detect and mitigate suspected spam or other unwanted messaging in real-time. CTIA's *Messaging Principles and Best Practices* call for different treatment of traffic based on volume, with more protections in place for consumers from high volume traffic. Once a message has been sent, providers' and their partners' spam filters and blocking techniques may enable providers to collect data about text messages, including message content (URLs, internet domains, etc.), for messages that are identified as potentially unwanted or harmful. This data can be used to adjust their sophisticated filters and algorithms to respond to evolving threats.

- **Targeted Blocking** – Providers employ targeted blocking of messages in a balanced approach aimed at protecting consumers from spam messages while also protecting legitimate messages. Providers may block texts if high-volume messages come from a sender that has not registered or is not using appropriate Non-Consumer messaging channels, or if providers have evidence that a message is unwanted. CTIA's *Messaging Security Best Practices* note that a risk assessment of unwanted messages may include, but is not limited to, network monitoring and evidence of fraud or other malfeasance, including fraud or malfeasance associated with compromised API credentials, utilization of grey routes, lack of authentication, or a pattern of abuse of industry best practices. Additionally, wireless providers use "account fingerprinting" techniques to identify accounts that are sending high volumes of messaging traffic with little or no voice or data usage. High volumes of messaging traffic often indicate the use of computer programs, such as a bot or other automated system, which are distributing unwanted messages.

- **Stopping Fraud at the Source** – Beyond registries, providers may have information about potential sources of unwanted messaging that can prevent them from being delivered to consumers. For example, providers may be able to identify the unique identifiers (e.g., telephone numbers), SIM cards, websites, and other information associated with spam campaigns and take action to suspend or shut down accounts and prevent bad actors from sending spam.

3. Consumer Mitigation

The Working Group considered consumer complaints as a significant source of information about unwanted messages. Sharing such information is helpful to spam mitigation. The

following describes ways that consumers can provide information about unwanted messages that can help stakeholders take action.

a. Consumer-Initiated Blocking

In addition to blocking tools employed within the ecosystem or mobile wireless networks, consumers also have the ability to identify and block unwanted messages. For example, wireless providers may offer solutions that enable consumers to block or "blacklist" messages from certain identifiers at the network level. Innovation is also occurring at the device level, where consumers can identify unwanted messages as "spam" or "junk" in native applications or add third-party applications that can filter and block unwanted text messages. Some industry stakeholders also offer the ability for consumers to block all texts that are not in a consumer's contact list.

b. Consumer Complaint Mechanisms

Consumers can forward unwanted messages to 7726 (SPAM). Information reported through 7726 is tracked, aggregated, and addressed by wireless providers and their ecosystem partners so they can further calibrate their spam filters and blocking tools, and enhance efforts to prevent unwanted messages. This may give providers more insight than, for example, reporting a robocall, because the information a consumer provides goes beyond the identifier (e.g., phone number) of the message sender.

In addition, there are vendors of security services that support messaging ecosystem stakeholders and consumers. These vendors offer spam message reporting solutions that a consumer can download or use on websites, such as SpamResponse.com. Spam records are cataloged in an internal database and could be used to update the security vendor's respective spam detection software and tools that are used by messaging ecosystem stakeholders.

Consumers may also report unwanted messages to the Commission and the FTC. Consumers may file a complaint with the Commission if they receive:[44]

- An unwanted commercial text message sent to their mobile phone;
- An autodialed text message sent to their mobile phone if they did not consent to the message previously (or it does not involve an emergency); and
- Any autodialed text message from a telecommunications company advertising its products or services, if sent without their consent.

The FTC advises consumers to report an unwanted text message as follows:

- Report it on the messaging app;

[44] FCC, Consumer Guide, Stop Unwanted Robocalls and Texts, Robotexts (last modified July 25, 2022), https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts.

- Copy the message and forward it to 7726 (SPAM); or
- Report it to the Federal Trade Commission at ReportFraud.ftc.gov.[45]

V. Considerations for the Commission

A. Encourage Broader Adoption of the Messaging Principles and Best Practices

The availability of industry best practices as they evolve enables messaging ecosystem stakeholders to minimize illegal and unwanted messages. As a result, the Working Group recommends that the Commission evaluate whether and how to encourage broader adoption of industry best practices among messaging stakeholders.

Importantly, CTIA's *Messaging Principles and Best Practices* place a strong emphasis on obtaining consumer consent and honoring consumer opt-out requests, similar to the TCPA's consent-based protections. Notably, the scope of messaging services to which CTIA's *Messaging Principles and Best Practices* applies is broader than the TCPA. As the U.S. Supreme Court has recently limited the scope of the TCPA, CTIA's *Messaging Principles and Best Practices* may encourage industry stakeholders to take steps to honor consumer consent more broadly than the application of the TCPA. The Commission should consider ways to encourage all industry stakeholders to employ CTIA's principles of requiring consent.

B. Education on How Consumers Can Protect Themselves from Unwanted Messages

While adoption and use of text messaging among consumers is commonplace, the Working Group observes that consumers are generally unaware of how to protect themselves from nefarious activity caused by unwanted and illegal text messages. The Working Group recommends that the Commission itself and with government partners, such as the FTC and state attorneys general, as well as other stakeholders, should enhance their efforts to ensure that consumers are aware of unwanted messaging solutions, including network and device-level message blocking tools, and how to report unwanted messages through 7726 (SPAM). Increasing consumer-initiated reporting through 7726 can help stakeholders take appropriate action and refine those capabilities to mitigate unwanted or illegal messages.

A coordinated public awareness campaign should provide similar information and use consistent language about how to identify unwanted or illegal text messages and steps that consumers should take to protect themselves by both blocking and reporting unwanted text messages. Public awareness campaigns should consider using a variety of mediums, such as social media platforms and Public Service Announcements distributed across broadcast, cable, and streaming video platforms. Public awareness campaigns should also ensure materials are available in multiple languages and accessible for people with a variety of disabilities, including deaf, hard of hearing, blind, low-vision, and cognitive disabilities.

[45] FTC, *How To Recognize and Report Spam Text Messages* (Feb. 2020), https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages#report.

VI. The Impact of Illegal Text Messages on Emergency Telephone Numbers

The Commission also asked the CAC to report on "whether and how illegal text messages pose a threat to emergency telephone numbers (e.g., PSAPs, hospitals, and other emergency institutions) and how the Commission can protect emergency call centers without negatively impacting legitimate emergency text messages." Telephone numbers that receive emergency communications, such as 911 and 988, may also be vulnerable to the effects of robotexts, but the Working Group did not find significant information about the scope of this issue or available solutions.

A. Institutions Affected

PSAPs that receive 911 emergency calls are notable targets for bad actors. The ability of PSAPs to receive text messages is relatively new. The first text-to-911 message was sent in 2009; that capability was supported by wireless providers nationwide by 2015.[46] PSAP adoption of text-to-911 services has been increasing, although not supported by every PSAP.[47] Because so many types of emergency calls go to the PSAPs – police, fire and rescue, medical emergency – keeping these sites free of the problems caused by robotexting is important.

Hospitals constitute another class of emergency institutions that receive text messages, independent of the 911 system. Their experience of robotext incursions, as noted below, is different from that of the PSAPs.

Other locations that receive critical text messages include the National Suicide Prevention Lifeline ("Lifeline"), as well as many of the associated local crisis centers. Today, consumers can text 988 to reach the Lifeline and affiliated local crisis centers throughout the U.S.[48] One source report indicates that the number of calls, texts, and chats to the hotline reached 96,000 between July 14 and July 20 – 30,000 more than the previous week.[49]

---

[46] *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications,* Second Report and Order and Third Further Notice of Proposed Rulemaking, 29 FCC Rcd 9846 (2014); Peter Svensson, *Iowa 911 center is first to accept text messages*, NBC News (Aug. 5, 2009), https://www.nbcnews.com/id/wbna32303244.

[47] FCC, Consumer Guides, Text to 911: What You Need to Know (last updated Jan. 6, 2020), https://www.fcc.gov/consumers/guides/what-you-need-know-about-text-911. A list of these locations is available at FCC, Public Safety, Policy and Licensing Division, 911 Services, PSAP Text-to-911 Readiness and Certification Registry (Text-to-911 Registry) (last updated July 15, 2022), https://www.fcc.gov/general/psap-text-911-readiness-and-certification-form.

[48] *See* News Release, FCC, *U.S. Transition to 988 Suicide & Crisis Lifeline Begins Tomorrow* (July 15, 2022), https://www.fcc.gov/document/us-transition-988-suicide-crisis-lifeline-begins-july-16; FCC, 988 Suicide and Crisis Lifeline (last updated July 20, 2022), https://www.fcc.gov/988-suicide-and-crisis-lifeline.

[49] *See* Julia Shapero, *National suicide hotline sees spike in calls with introduction of 988 number*, Axios (July 22, 2022), https://www.axios.com/2022/07/22/national-suicide-hotline-sees-spike-calls-988-number.

B. Types of Threats

Robotexts, like voice robocalls, pose more than one kind of potential harm to emergency institutions.

In 2020, the Commission established a working group specifically tasked with addressing potential harm to hospitals, the Hospital Robocall Protection Group ("HRPG").[50] A report from the HRPG summarizes different types of unlawful robocalls.[51] From these types we can extract general categories of threats posed by robocalls or robotexts.

- **Volume** – An excessive number of texts to an emergency institution may overwhelm the site's answering capacity, impairing its ability to carry on its normal activities. The effect is similar to that of a distributed denial-of-service attack on an information system.[52]

- **Fraud** – Like voice calls, robotexts can be used for fraudulent purposes, including phishing, "social engineering" attempts to obtain sensitive information, and scams generally.[53] While much of the discussion of such frauds focuses on voice calls rather than texts, the text problem may actually be greater than the phone call problem. One source estimates that the average smartphone user in the U.S. receives 28 spam calls, but 42 spam texts, per month.[54]

- **Privacy** – The fraud issue overlaps with privacy concerns, where phishing robotexts to institutions may be used to obtain individuals' personal information, possibly leading to identity theft.[55] It is unclear whether the emergency institutions could be legally liable for the disclosure of personally identifiable information.

C. Extent of the Threats

The information available to the CAC so far suggests that the size of the problem may differ for different types of emergency institutions and types of communications methods. No data were available to the Working Group on text message-based problems or threats to emergency institutions.

As a result, it appears that PSAPs may be largely unaffected, so far. For example, one emergency center in Fairfax County, Virginia, reported receiving only three to five text messages a day, on average. Even when a larger number (say, fifteen in one day) are received, this larger number of texts tends to come from individuals with behavioral issues, rather than from bots or

---

[50] FCC, *Hospital Robocall Protection Group (HRPG)*, at 4 (2020) ("HRPG Report"), https://www.fcc.gov/-sites/default/files/hrpg_report.pdf.

[51] *Id*. at 6-8.

[52] *See id*. at 5, 6-7.

[53] *Id*. at 7.

[54] Heather Kelly, *The nonstop scam economy is costing us more than just money*, Wash. Post (July 13, 2022), https://www.washingtonpost.com/technology/2022/07/13/scam-fraud-fatigue/ (citing data from the RoboKiller app).

[55] HRPG Report at 6.

automatic senders.[56] While the volume of texts-to-911 may grow as people become more familiar with that capability, at this stage robotexts to PSAPs do not seem to be a significant problem.

Robotexts to hospitals, on the other hand, may constitute a problem. The HRPG Report states, "Hospitals receive fraudulent, disruptive and nuisance robocalls flooding communication networks and annoying calls to patient rooms."[57] The report does not distinguish between voice calls and text messages, and it is possible the text side of the equation does not yet present major issues. The Commission may wish to consult with the HRPG, or seek public comment, about the prevalence of spurious text messages to hospitals.

D. Protecting Emergency Institutions

The Commission may wish to monitor the issue.

In dealing with emergencies, the need to avoid false positives (legitimate texts that are incorrectly blocked as unlawful) is greater than in non-emergency cases. It would certainly be undesirable if individuals in real difficulty were unable to reach a 911 answering center because an algorithm judged the text to be spam. The downside of false positives must be taken into account in evaluating any potential remedies.

VII. Accessibility Considerations for the Commission

The FCC asked the CAC to provide "data and other information describing…how the Commission should take into account accessibility concerns when developing solutions to combat unwanted text messages." Per the Commission, federal law requires advanced communications services, like text messages, to be "accessible and usable by people with disabilities."[58]

People with disabilities, including the deaf, hard of hearing, and people with speech disabilities, were early adopters of SMS and MMS. Based on usage data and consultations with experts, SMS and MMS are accessible and widely used across every demographic group.[59] Accessibility

[56] Conversation with the Department of Public Safety Communications at Fairfax County, July 12, 2022.

[57] HRPG Report at 5.

[58] The FCC notes that, "[t]o be *accessible*, the main functions of a product or service must be locatable, identifiable and operable by individuals with varying abilities, and all information necessary to operate and use the product or service must have an accessible output or display." Further, the Commission has stated that, "[t]o be *usable*, individuals with disabilities must be able to learn about and operate the product or service's features, and must be able to access information and documentation for the product or service, including instructions and user guides. *See* FCC, Consumer Guides, Accessibility of Advanced Communications Services and Equipment (last updated Jan. 27, 2021), https://www.fcc.gov/consumers/guides/accessibility-advanced-communications-services-and-equipment (citing the Twenty-First Century Communications and Video Accessibility Act).

[59] *See, e.g.,* Nathan W. Wood et al., *Wireless Device Use by Individuals with Disabilities: Findings from a National Survey*, Journal on Technology and Persons with Disabilities (2020) ("*Wireless Device Use by Individuals with Disabilities*"), https://scholarworks.csun.edu/bitstream/handle/10211.3/215988/2203%20Survey%20of%20User%20Needs%20for%20Wireless%20Devices%20Key%20Findings.pdf?sequence=1; Andrew Perrin, *Mobile Technology and Home*

concerns in the context of unwanted text messaging revolve primarily around ensuring that Commission efforts to educate the public about how to recognize and respond to illegal text messaging are sufficiently inclusive.

As discussed in more detail below, the Working Group finds that:

- Conversations regarding technology accessibility tend to focus primarily on people with disabilities. In the context of illegal text messages, these conversations should also encompass older adults, a community that benefits from many of the accessibility solutions and related educational efforts developed to assist people with disabilities in their uses of advanced communications services.

- Currently, it does not appear that illegal and unwanted texts are any more of a problem among people with disabilities or senior citizens than with the overall U.S. population.

- Commission efforts to address accessibility issues in the context of illegal and unwanted text messages should focus primarily on ensuring that its education and outreach activities are tailored to meet the needs of people with disabilities community and senior citizens.

A. Accessibility Concerns Implicate More than Just People with Disabilities

As a threshold matter, the Working Group observes that accessibility concerns in the context of illegal and unwanted text messages implicate more than just people with disabilities. Experts consulted by the Working Group noted that the technology accessibility needs of older adults often overlap with those of people with disabilities, in large part because seniors are more likely than any other age group to report a disability. Data from the CDC indicate that 40% of adults aged 65 years and older have a disability.[60] Accordingly, accessibility solutions developed for people with certain kinds of disabilities – e.g., screen readers for the vision impaired; the ability to enlarge text on a smartphone; read-aloud applications – have also benefitted seniors.

A similar dynamic is evident vis-à-vis educational efforts aimed at informing these communities of potential risks arising from their uses of technology. Experts indicated that the techniques used to design education campaigns for people with disabilities will likely be useful in similar campaigns for older adults. The use of plain language was cited by several experts as a critical component of successful education and outreach efforts in both communities.

Plain language describes writing that is clear, concise, allows readers to "find what they need, understand what they find the first time they read or hear it," and "use what they find to meet

Broadband 2021, Pew Research Center (June 3, 2021), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/06/PI_2021.06.03_Mobile-Broadband_FINAL.pdf.

[60] CDC, Disability Impacts us All, https://www.cdc.gov/ncbddd/disabilityandhealth/infographic-disability-impacts-all.html (last updated Sept. 16, 2020).

their need."[61] Implicit in this definition is the importance of writing and developing materials with a particular audience in mind. The plain language used in materials designed for the general population, for example, might still be too complex for certain segments. As noted below, refining materials regarding spam texts, and boiling down concepts even further, may be appropriate for use among people with certain kinds of disabilities and among seniors who are new to mobile technologies.

B. Text Messaging is Popular Among People with Disabilities and Seniors, but Spam Texting Does Not Currently Appear to be a Major Issue for These Groups

The intuitive nature of texting, along with technology solutions developed to make SMS and MMS broadly accessible, has resulted in text messaging being widely used among people with disabilities and among senior citizens. As in most other demographic groups, these communities are using texts to communicate with family and friends and receive important information from businesses and healthcare providers.[62]

In recognition of the growing popularity of smartphones and texting among people with disabilities and seniors, several organizations have leveraged SMS/MMS to deliver targeted services. For example, the National Disability Institute launched a texting campaign during the pandemic to deliver messages to "help combat stress and feelings of isolation, build positive thinking and establish new behavior patterns that promote emotional well-being and financial resilience."[63] Similarly, AARP uses texts to regularly deliver information on a range of topics and initiatives via its 22777 short code.[64] In both cases, participants were required to opt into the campaign.

Experts consulted by the Working Group who work with people with disabilities and older adults noted that, even though use of text messaging is high among those who have adopted the technology, spam texting issues do not appear to be more prevalent among seniors or people with disabilities than among all other consumers.

C. Commission Efforts to Address Accessibility Concerns Should Focus on Assuring Tailored Education and Outreach

Efforts by the Commission to educate consumers about the threats associated with illegal text messages and equip them with the tools needed to combat spam texts should be accessible by as many people as possible. Experts consulted by the Working Group stressed the importance of

---

[61] PlainLanguage.gov, Federal Plain Language Guidelines, https://www.plainlanguage.gov/guidelines/ (last visited Aug. 17, 2022). Producing educational materials in plain language could also have benefits for people with cognitive disabilities.

[62] *See, e.g.*, *Wireless Device Use by Individuals with Disabilities*

[63] NDI, *National Disability Institute Launches Text Campaign to Promote Stress Reduction and Financial Resilience for People with Disabilities and Chronic Health Conditions*, https://www.nationaldisabilityinstitute.org/press/ndi-launches-resilientpwd-text-campaign/ (last visited Aug. 17, 2022).

[64] *See, e.g.*, AARP, *Get Plugged in Via Text Messages*, https://states.aarp.org/montana/receivetextalerts (last visited Aug. 17, 2022).

building accessibility into relevant materials from the outset and then tailoring outreach activities to reflect the needs of discrete communities.

The use of plain language in educational materials can assist in assuring a baseline of accessibility. Breaking relevant issues into smaller pieces could also help in effectively communicating what a spam text is, what it might look like, the harms arising from engaging with a spam text, and the methods available to combat them. Such an approach will also resonate with consumers who possess a lower level of technological expertise.

Regarding effective outreach, experts stressed the importance of targeted engagement. The Commission might consider reaching out to disability-specific groups and those representing seniors to solicit their feedback regarding additional resources that might be needed to raise awareness about spam texting. Experts highlighted the value of leveraging existing channels for doing this. For example, the Commission might work with Senior Planet from AARP to directly engage older adults on these issues. Similarly, the Commission might partner with the American Council of the Blind ("ACB") to sponsor a program on its radio show (www.acbradio.org) dedicated to the issue of illegal text messages. These efforts might be supplemented with tailored educational materials that build on those developed for the general population. For example, materials developed in partnership with the ACB might walk a consumer through the process of using assistive technologies to copy and paste a spam text and send it to 7726. Similar efforts could be deployed to assure robust engagement with people with other disabilities (e.g., those who are deaf or hard of hearing; those with cognitive disabilities; etc.) and seniors.

VIII. CONCLUSION

The Consumer Advisory Committee appreciates the opportunity to provide its input to the Commission on this important consumer protection topic. Should the Commission have additional questions or concerns, members of the CAC would be happy to provide additional information to examine the problem of illegal and unwanted text messages.

[Adopted by the Consumer Advisory Committee – August 30, 2022]

Respectfully Submitted,

Steve Pociask, CAC Chair

Debra Berlyn, CAC Vice-Chair

Appendix A

Experts Consulted by the Working Group

- American Council of the Blind
- AT&T
- CTIA
- Fairfax County, VA, Department of Public Safety Communications
- Federal Communications Commission
- National Consumer Law Center
- Older Adults Technology Services (OATS) from AARP
- Twilio

Appendix B

Text Blocking Working Group Members

- Michael Santorelli (serving individually)
- Steve Pociask, American Consumer Institute
- Vonda Long, AT&T
- Linda Vandeloop, AT&T (alternate)
- Sarah Leggin, CTIA
- Amy Bender, CTIA (alternate)
- Joslyn Day, Massachusetts Department of Telecommunications and Cable
- William Bendetson, Massachusetts Department of Telecommunications and Cable (alternate)
- Thaddeus Johnson, National Association of State Utility Consumer Advocates
- Rick Ellrod, National Association of Telecommunications Officers and Advisors
- Margot Saunders, National Consumer Law Center
- John Breyault, National Consumers League
- Eden Iscil, National Consumers League
- Debra Berlyn, Project GOAL