Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS ON NOTICE OF PROPOSED RULEMAKING IN CG DOCKET NO. 21-402

by

Electronic Privacy Information Center
National Consumer Law Center on behalf of its low-income clients
Consumer Action
Consumer Federation of America
National Association of Consumer Advocates
National Consumers League
Public Knowledge
U.S. PIRG

Submitted November 10, 2022

Chris Frascella
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

Margot Saunders
Senior Counsel
National Consumer Law Center
1001 Connecticut Avenue, NW
Washington, DC 20036

Summary

The **Electronic Privacy Information Center (EPIC)**, and the **National Consumer Law Center (NCLC)** on behalf of its low-income clients, along with **Consumer Action**, **Consumer Federation of America, National Association of Consumer Advocates, National Consumers League, Public Knowledge**, and **U.S. PIRG**, file these comments to encourage the Federal Communications Commission ("Commission" or "FCC") to prioritize protecting consumers from widescale nuisance and fraud facilitated through unwanted and illegal text messages placed through the U.S. telephone network.

We urge the Commission to extend additional protections for consumers from illegal and unwanted robotexts. The different types of robotexts that harm consumers require different mechanisms to address them. We recommend that the Commission—

1) Protect consumers from illegal telemarketing texts by clarifying its own regulations in a way that that would dramatically reduce the number of texts that violate these rules.

2) Ensure that the voluntary efforts employed by CTIA and its industry partners to place meaningful limits on unwanted texts sent by law-abiding groups for fundraising, political, survey, or other purposes remain effective.

3) Prioritize the development of ways to eliminate scam texts, especially those that include URLs. Scam robotexts often contain malware that leads to imposter websites to solicit personal information from the subscriber used for theft of funds from bank accounts, identity theft, and other scams.

Additionally, we urge the Commission to consider how it might protect consumers from non-SMS text messaging, such as iMessage, and scams perpetrated over other messaging apps.

Table of Contents

Comments

I. Introduction – Different of types of text messages cause different harms.

The **Electronic Privacy Information Center (EPIC)**, and the **National Consumer Law Center (NCLC)** on behalf of its low-income clients, and **Consumer Action**, **Consumer Federation of America, National Association of Consumer Advocates, National Consumers League, Public Knowledge**, and **U.S. PIRG** file these comments to encourage the Federal Communications Commission ("Commission" or "FCC") to prioritize protecting consumers from widescale nuisance and fraud facilitated through unwanted and illegal text messages placed through the U.S. telephone network. We appreciate the Commission's recognition of the problem and its initiation of this proceeding to address it. In furtherance of the Commission's efforts to address the surge of unwanted and illegal texts, we urge several additional steps to stop these texts from reaching subscribers.

In this Proposed Rule,[1] the Commission proposes mandatory network-level blocking of texts sent from a Do Not Originate (DNO) list.[2] This appears to us to be a good proposal, but it is not nearly sufficient to address the escalating threat that scam texts, and other illegal texts, which pose risks to subscribers and the cell phone network. Unless meaningful action is taken soon, the subscribers' trust in text messages will be irretrievably broken, as has become the case with voice calls.[3]

---

[1] *In re* Targeting and Eliminating Unlawful Text Messages, Notice of Proposed Rulemaking in CG Docket No. 21-402, 87 Fed. Reg. 61,271 (Oct. 11, 2022), *available at* https://www.federalregister.gov/documents/2022/10/11/2022-22049/targeting-and-eliminating-unlawful-text-messages [hereinafter Proposed Rule].

[2] *Id.* at 61,271 ¶ 1.

[3] Seventy percent of phone subscribers no longer answer the phone for numbers they do not recognize. *See* Octavio Blanco, Consumer Reports, Mad About Robocalls? (Apr. 2, 2019), *available at* https://www.consumerreports.org/robocalls/mad-about-robocalls/.

There are different types of robotexts that harm consumers, each with potentially different mechanisms necessary to address them. These include:

1. **Telemarketing texts to numbers on the do-not-call (DNC) registry.** The Telephone Consumer Protection Act (TCPA) already provides some redress to consumers who receive texts in violation of the regulations issued pursuant to 47 U.S.C. § 227(c). However, as we describe in section II, *infra*, and we have explained in previous filings,[4] there are simple clarifications that the FCC can make regarding the interpretations of the regulations that could dramatically reduce the number of texts that violate these rules.

2. **Unwanted texts sent by law-abiding groups for fundraising, political, survey, or other purposes.** These texts involve neither telemarketing nor outright scams, but are typically requests for political engagement or contributions, surveys, or similar messages. The efforts employed by CTIA and its industry partners currently provide a degree of mitigation of the nuisance and invasion of privacy caused by these messages. The Commission should take care not to inhibit these measures.

3. **Scam robotexts, some of which utilize URLs.** Scam robotexts can contain malware that leads to imposter websites to solicit personal information from the subscriber used for theft of funds from bank accounts, identity theft, and other scams. The Commission must expand its efforts to eliminate these messages.

Additionally, in section V, *infra*, we urge the Commission to consider how it might protect consumers from non-SMS text messaging, such as iMessage, and scams perpetrated over other messaging apps.

[4] *See, e.g.,* Notice of *Ex Parte* Presentation, National Consumer Law Center et al., CG Docket No. 02-278 Report No. 3170–relating to the limits on Exempt Calls to clarify that that prerecorded scam calls and automated scam texts are not exempt from TCPA consent requirements; and in the Matter of Assurance IQ, LLC's Petition, DA 20-540 (Oct. 4, 2022), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/1005271665623 [hereinafter Notice of *Ex Parte* Presentation Oct. 4, 2022].

II. The Commission should reiterate and enforce the requirement that prior express invitation or permission to receive telemarketing calls and texts can be given to only one seller at a time.

We have a reasonably accurate estimate of the number of telemarketing calls and scam *calls* made each month because of the analytics provided by companies like YouMail,[5] but do not have data showing the full volume of telemarketing texts. Yet we know from complaints to the FCC that the numbers are increasing.[6]

Under the FCC's nationwide DNC rule,[7] telephone solicitations (defined by 47 U.S.C. § 227(a)(4)), cannot be made to residential telephone numbers that are registered on the DNC Registry unless the subscriber has provided "prior express invitation or permission" that "clearly authorizes the seller" to make the call or cause it to be made, or the telemarketer making the call "has a personal relationship with the recipient."[8] This prohibition applies not just to land lines, but also to cell phones, which are presumed to be residential.[9] Since text messages are treated as calls for purposes of the TCPA,[10] the result is that telemarketing text messages are subject to the nationwide DNC rule in all respects, and cannot be sent to a number on the DNC Registry without the called party's prior express invitation or permission.

---

[5] *See* PR Newswire, U.S. Phones Received 4.2 Billion Robocalls in September, Says YouMail Robocall Index (Oct. 5, 2022), *available at* https://www.prnewswire.com/news-releases/us-phones-received-4-2-billion-robocalls-in-september-says-youmail-robocall-index-301641224.html.

[6] *See In re* Targeting and Eliminating Unlawful Text Messages, Notice of Proposed Rulemaking, CG Docket No. 21-402, at ¶ 3 (F.C.C. Rel. Sept. 27, 2022), *available at* https://docs.fcc.gov/public/attachments/FCC-22-72A1.pdf.

[7] 47 CFR § 64.1200(c). *See In re* Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, Report and Order, CG Docket No. 02-278, 18 F.C.C. Rcd. 14014 (F.C.C. July 3, 2003).

[8] 47 C.F.R. §§ 64.1200(c)(2)(ii), (iii), (f)(9).

[9] 47 C.F.R. § 64.1200(e).

[10] *See, e.g.*, Pariseau v. Built USA, L.L.C., ___ F. Supp. 3d ___, 2022 WL 3139243, at *2 (M.D. Fla. Aug. 5, 2022) (text message is a call for purposes of do-not-call rule).

Two major problems undermine the effectiveness of the DNC rule for both voice calls and text messages. First, as illustrated by a case recently filed by the Pennsylvania Attorney General, "lead generation" companies use websites luring consumers with promises of rewards and sweepstakes to trick them into providing their contact information.[11] As described in that case, consumers enter their contact information on a website and, when they apply for the prize, that button is hyperlinked to a long list of unrelated callers or sellers. The lead generator then sells the consumer's contact information to telemarketers. If the consumer complains or files suit regarding the resulting barrage of unwanted telemarketing calls, the caller or seller claims prior express invitation or permission as a defense.[12] But the consumer has not actually provided permission to the particular caller, or for calls related to the product being sold. Instead, the permission was often obtained through a hyperlink on an unrelated website.

In an *ex parte* we recently filed with the Commission, we provided an illustration of what happens when a consumer applies online for information about car insurance.[13] In that example, after the consumer inputs their contact information and the telephone number, they are invited to click on a large button that says GET MY AUTO QUOTES. But, below the GET MY AUTO QUOTES button, the following appears—in a tiny font:

> By clicking the button above, I consent to receive emails, calls and/or text messages, for marketing purposes, regarding insurance quotes, or other products and services on behalf of Free-insurance-quotes.us partners, using my provided telephone number even if it's on a federal, state or corporate do-not-call list. I acknowledge calls may be pre-recorded messages using artificial voice and/or placed using an automated telephone dialing system. I understand consent is not required to purchase and that I may revoke my consent at any time. Applicable text messaging rates may apply. I agree to the Privacy Policy and Terms of Service provided.

[11] Complaint, Commonwealth of Pennsylvania by Josh Shapiro, Attorney General v. Fluent, L.L.C., No. 2:22-cv-1551 (W.D. Pa. Nov. 2, 2022), *available at* https://www.attorneygeneral.gov/wp-content/uploads/2022/11/Commonwealth-of-PA-v.-Fluent-LLC-et-al..pdf.

[12] *See id.* at ¶¶ 26, 28, 30.

[13] Notice of *Ex Parte* Presentation Oct. 4, 2022, *supra* note 4.

The weblink attached to the words "Free-insurance-quotes.us. partners" includes a list of 8,422 different sellers of products or services, the majority of which are not related to insurance.[14]

The commonality of this fact pattern is reflected in several large cases winding their way through the courts,[15] all of which are about hundreds of millions of unwanted and invasive telemarketing calls and texts that continue to plague the cell phones of American subscribers.

Yet, obtaining prior express invitation or permission in this way does not comply with the Commission's existing rules, which allow invitation or permission to be provided to just one seller at a time:

> Any person or entity making telephone solicitations (or on whose behalf telephone solicitations are made) will not be liable for violating [the nationwide DNC rule] if:
> …
> (ii) It has obtained the subscriber's prior express invitation or permission. Such permission must be evidenced by a signed, written agreement *between the consumer and seller* which states that the consumer agrees to be contacted by *this* seller . . . .[16]

If the "one seller at a time" rule were enforced by the FCC, it would greatly reduce the number of unwanted telemarketing calls and text messages that consumers receive. It would prevent lead generators from tricking consumers into purportedly assenting to receive calls from long lists of sellers and telemarketers, and it could be the basis for telecom providers blocking many of these unwanted messages.

---

[14] *Id.* at 12.

[15] *See, e.g.,* McCurley v. Royal Seas Cruises, Inc., 2022 WL 1012471 (9th Cir. Apr. 5, 2022) (Rejecting consent defense based on leads from a third party because of significant amounts of mismatched data).*See also* Pesach Lattin, *Performance Marketing Insider, Bot Form Fills are Destroying Lead Generation Industry. What Can be Done?* (Mar. 19, 2019), *available at* https://performinsiders.com/2019/03/bot-form-fills-are-destroying-lead-generation-industry-what-can-be-done/ [hereinafter Lattin, *Bot Form Fills*]; Alexandra Bruell, *Fraudulent Web Traffic Continues to Plague Advertisers, Other Businesses*, The Wall St. J., Mar. 8, 2018, *available at* https://www.wsj.com/articles/fraudulent-web-traffic-continues-to-plague-advertisers-other-businesses-1522234801 [hereinafter Bruell, *Fraudulent Web Traffic*]; Josh Sternberg, Digiday, *Confessions of a Lead-Gen Specialist* (June 4, 2012), *available at* https://digiday.com/marketing/confessions-of-a-lead-gen-specialist/ [hereinafter Sternberg, *Confessions of a Lead-Gen Specialist*].

[16] 47 C.F.R. § 64.1200(c)(2)(ii) (emphasis added).

The second major problem is that prior express invitation or permission is often manufactured out of whole cloth by unscrupulous lead generators and data brokers.[17] For example, a recent decision documents how a lead generator apparently pirated another company's website in order to generate or falsify the source of leads.[18] Another technique is to obtain consumer contact information through various other means, and then manipulate the data to appear as if it had been entered on a consent form by the consumer.[19] Bots may fill out consent forms. Or the entities involved in the scam may alter consent forms after the fact. For example, a complaint filed by the Ohio Attorney General against callers making the ubiquitous auto warranty calls noted that:

> when a VoIP Provider of Sumco Panama had to respond to an ITG traceback request, Sumco Panama needed to "buy some time" before responding in order to *add* "auto services" language to the list of opt-in websites in the terms and conditions *after* many VSC robocalls were made based on the alleged "opt in" from these websites."[20]

To address these problems, we urge the Commission to:

1. Issue a declaration reiterating the DNC rule's provision that express invitation or permission can be given to only one seller at a time.

2. Bring enforcement proceedings against telemarketers and sellers that make calls based on purported consent that was provided in bulk to a list of callers.

---

[17] *See* Lattin, *Bot Form Fills*, *supra* note 15; Bruell, *Fraudulent Web Traffic*, *supra* note 15.

[18] Mantha v. Quotewizard.com, L.L.C., 2021 WL 6061919, at *9 (D. Mass. Dec. 13, 2021), *adopted by* 2022 WL 325722 (D. Mass. Feb. 3, 2022).

[19] *See also* Lattin, *Bot Form Fills*, *supra* note 15; Bruell, *Fraudulent Web Traffic*, *supra* note 15; Sternberg, *Confessions of a Lead-Gen Specialist*, *supra* note 15.

[20] Complaint, State of Ohio *ex rel.* Attorney General Dave Yost v. Jones et al., No. 22-cv-02700, at ¶ 69 (S.D. Ohio July 7, 2022), *available at* https://www.ohioattorneygeneral.gov/Files/Briefing-Room/News-Releases/Time-Stamped-Complaint-22-CV-2700-State-of-Ohio-v.aspx (italics in original; underlining added).

3. Promptly deny the petition filed by Assurance IQ, LLC that is pending before the Commission.[21] Granting Assurance's request for a free pass on making unwanted calls when it claims a reasonable basis for believing it had consent would fly in the face of the widespread evidence of ineffective consent and fraudulently manufactured consent. It would remove all incentives for callers to scrutinize the alleged consent obtained by lead generators, and encourage a head-in-the-sand approach that would allow fraud and overreaching to flourish.[22]

III. The Commission must ensure the continuance of industry's best practices and requirements for consent for robotexts.

The primary means that consumers have long had to protect themselves from mass texts is the prohibition against sending a text using an automated telephone dialing system (ATDS)[23] to a cell phone without prior consent.[24] However, many courts, interpreting the decision by the U.S. Supreme Court in *Facebook, Inc. v. Duguid*,[25] have held that the systems used to send mass texts do not fit within the TCPA's definition of an ATDS. While we disagree with those decisions, and are participating as *amici* opposing that interpretation, those decisions have emboldened the *en masse* senders of unwanted text messages. Although the nationwide DNC rule still protects cell phones from unwanted telemarketing text messages, if the ATDS definition is interpreted not to apply to mass automated texting systems, no consent requirement will apply to non-telemarketing text messages, and consumers will have no legal right to make them stop.

---

[21] *See* Public Notice, Federal Commc'ns Comm'n, Consumer and Governmental Affairs Bureau Seeks Comment on Petition for Declaratory Ruling Filed by Assurance IQ, LLC, CG Docket No. 02-278, DA 20-540 (Rel. May 21, 2020), *available a*t https://docs.fcc.gov/public/attachments/DA-20-540A1.pdf.

[22] *See* Notice of *Ex Parte* Presentation Oct. 4, 2022, *supra* note 4, at 8-10 (spelling out our response to the Assurance petition in more detail).

[23] 47 U.S.C. § 227(a)(1).

[24] 47 U.S.C. § 227(b)(1)(A)(iii).

[25] 592 U.S. ___, 141 S. Ct. 1163, 209 L. Ed. 2d 272 (2021).

Fortunately, the telecom providers and their trade associations have provided a measure of relief in this space. Recognizing that telecom providers benefit when their customers are happy with their services, and that consumers overwhelmingly want to receive only those texts for which they have provided consent,[26] CTIA and the major cell phone providers have established voluntary registries for mass texters. Senders who use a registry to send mass texts must abide by registry rules, including requiring that the sender have consent from the recipient for the texts and that the texts contain a "stop" mechanism, which informs recipients that they can request that texts from that text sender no longer be sent.[27] In return for using the registry for text campaigns,[28] text senders are charged less for registry-compliant messages than text campaigns that are not sent through the registry.[29] By offering discounted prices for texts sent in compliance with their rules,[30] the registry gives an incentive to text senders to use the registry. The registry blocks texts sent through the registry that violate its security standards.[31]

The practices that this system promotes are voluntary, and the rules the CTIA and its partners have developed apply only to texts sent through their registries. There is no rule or

---

[26] *See* CTIA, Political Text Messaging: Engaging and Organizing Voters While Protecting Consumers (July 21, 2022), *available at* https://www.ctia.org/news/political-text-messaging-engaging-and-organizing-voters-while-protecting-consumers.

[27] *See* CTIA, Messaging Principles and Best Practices 15 (July 2019), *available at* https://api.ctia.org/wp-content/uploads/2019/07/190719-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf.

[28] Campaign Registry, About The Campaign Registry, *available at* https://www.campaignregistry.com/what-is-campaign-registry/ .

[29] *See* Emily Champion, Bandwidth Support Center, 10 DLC Overview (updated Mar. 2022), *available at* https://support.bandwidth.com/hc/en-us/articles/1500002422242. Compare $0.003 per message for registered traffic with $0.004 per message for unregistered traffic at T-Mobile, and $0.004 for unregistered and $0.002 for registered at AT&T.

[30] *See id.* Compare $0.002 for political messaging with $0.003 for insurance agents.

[31] *See* CTIA, Managing Security Best Practices (June 2022), *available at* https://api.ctia.org/wp-content/uploads/2022/06/Messaging-Security-Best-Practices-June-2022.pdf [hereinafter CTIA Best Practices].

mechanism that requires participation in CTIA's best practices for registries. While wireless carriers have their own security protocols, if the text campaigns are not sent through the registry process, the automated text messages will not be certified by the sender to have consent from the recipient, may not contain a "stop" mechanism, or may violate the security protections employed by the wireless carriers.[32] Text scammers have no reason to follow these registry rules, and every reason to evade them.

The importance of the voluntary best practices and registries employed by the carriers cannot be overstated. These practices go a long way toward providing consumers with meaningful limits on unwanted text messages from law-abiding texters. It is essential, therefore, that the FCC ensure that these voluntary efforts remain supported and facilitated by the regulatory regime it promulgates to stop illegal and unwanted texts.

IV. The Commission must take strong action against scam robotexts.

While some scam texts are likely to be prevented from reaching consumers because of the industry's protocols, the ongoing rise in consumer losses from scam texts indicate that these voluntary practices are not, by themselves, sufficient to stop scam texts.

The harms from text-based scams are significant. The FTC documented $131 million dollars from consumer-reported losses from text message-based scams in 2021, with a median loss of $900.[33] This is itself a significant increase over the FTC's 2020 loss figures.[34] Yet, the FTC's number

---

[32] *See id.*

[33] Federal Trade Comm'n, Consumer Sentinel Network Data Book 2021, at 12 (Feb. 2022), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf. Note that these figures do not distinguish between text-based robocalls and live text communications.

[34] Federal Trade Comm'n, Consumer Sentinel Network Data Book 2020, at 12 (Feb. 2021), *available at* https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf (noting $86MM in consumer-reported losses with a median loss of $800 per 2020 data). $131MM is a more than 52% increase over $86MM.

is much lower than the actual number, as many consumers do not report their losses. As we noted earlier this year, the FTC's consumer-reported losses from scam texts have exploded since 2017, an increase of 315% in the number of complaints and 254% in reported losses.[35]

The Commission points out that implementing measures to stop unwanted and illegal texts will have direct monetary benefits to consumers. The Commission seeks comment on its measurement of these estimated benefits.[36] We believe that the benefits from eliminating many of these texts are actually much higher than those identified by the Commission. The Commission estimates a current cost to consumers of $4.3 billion in nuisance texts ($0.05 per call for 86 billion calls) and $2 billion in direct consumer losses from fraud (20% of its $10.5 billion estimate of robocall harm).[37] However, the Commission's $10.5 billion figure for direct losses comes from a 2019 Truecaller report.[38] If Truecaller's 2022 number is applied to the Commission's 20% estimate, the updated 2022 numbers show that the total losses from scam robocalls go up to approximately $39.5 billion, once 20% is applied to that figure, there are $7.9 billion in losses from scam texts.[39]

---

[35] National Consumer Law Center & Electronic Privacy Information Center, Scam Robocalls: Telecom Providers Profit 10 (June 2022), *available at* https://www.nclc.org/wp-content/uploads/2022/09/Rpt_Scam_Robocalls.pdf.

[36] Proposed Rule, *supra* note 1, at 61,274 ¶ 26.

[37] *Id.*

[38] *See In re* Call Authentication Trust Anchor Implementation of TRACED Act section 6(A) – Knowledge of Customers by Entities with Access to Numbering Resources, Report and Order and Further Notice of Proposed Rulemaking, WC Docket Nos. 17-97, 20-67, 35 FCC Rcd. 3241, 3263 ¶ 48 (Mar. 31, 2020) (per TrueCaller 2019 Survey data).

[39] Truecaller, Truecaller Insights 2022 U.S. Spam & Scam Report (May 24, 2022), *available at* https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report. Note that the Commission's $4.3 billion in estimated nuisance costs, which reflects non-scam telemarketing texts as well, would still need to be added to this, for an annual benefit floor of $12.2 billion rather than $6.3 billion. However, even this number perhaps should be larger. RoboKiller, The RoboKiller Report, 2022 Mid-Year Phone Scam Insights, *available at* https://www.robokiller.com/the-robokiller-report#Robotexts-are-increasingly-out-of-control (Robokiller also estimates that more than nine billion spam texts are sent per month, suggesting that a nuisance cost based upon 100+ billion messages, rather than 86 billion, would be more reflective of the current reality experienced by phone subscribers). *See also* RoboKiller, 2022 United States robotext trends, *available at* https://www.robokiller.com/spam-text-insights.

Adding the nuisance costs to the updated direct losses yields a total annual benefit of $12.2 billion. We urge the Commission to use a more up-to-date estimate for consumer losses, which will then illustrate much greater benefits from implementing aggressive measures against unwanted and illegal texts.

Scam texts containing URLs are particularly risky to consumers, as URLs can trigger malware or the placement of apps on the recipient's cell phone that can directly lead to consumer losses.[40] The FCC and the Federal Trade Commission have each issued warnings not to click links in suspicious text messages.[41] The danger of URLs is highlighted by the fact that, indeed, software being sold facilitates the creation and distribution of malicious URLs as a tool to assist scammers looking to run SMS-based campaigns.

The dangers of scam texts containing URLs are illustrated by the experience of a victim who reached out to NCLC for assistance. She had received a text, which appeared to be from her bank, asking if she had recently authorized a $1500 transfer, and instructed that, if not, she should click on the provided URL. Once she clicked on the URL, an instant pay app was installed on her phone,

---

[40] *See, e.g.,* Hank Schless, Lookout, *Malware as a Service Meets Mobile Phishing: A Dangerous Combo* (Apr. 27, 2021), *available at* https://www.lookout.com/blog/flubot-malware-as-a-service-meets-mobile-phishing [hereinafter Schless, *A Dangerous Combo*]. There is also reason to believe similar tools are being used for IRS fraud. *See* Press Release, Internal Revenue Serv., IRS reports significant increase in texting scams; warns taxpayers to remain vigilant (Sept. 28, 2022), *available at* https://www.irs.gov/newsroom/irs-reports-significant-increase-in-texting-scams-warns-taxpayers-to-remain-vigilant [hereinafter IRS Press Release] (quoting IRS Commissioner Chuck Rettig as saying "This is phishing on an industrial scale so thousands of people can be at risk of receiving these scam messages" and "In recent months, the IRS has reported multiple large-scale smishing campaigns that have delivered thousands – and even hundreds of thousands – of IRS-themed messages in hours or a few days, far exceeding previous levels of activity.").

[41] Federal Commc'ns Comm'n, How to Identify and Avoid Package Delivery Scams, *available at* https://www.fcc.gov/how-identify-and-avoid-package-delivery-scams ("In some cases, a link may open a website that prompts you to enter personal information, or it may install malware on your phone or computer that can secretly steal personal information."); Rosario Mendez, Federal Trade Comm'n, Don't click links in unsolicited text messages (Apr. 27, 2020), *available at* https://consumer.ftc.gov/consumer-alerts/2020/04/dont-click-links-unsolicited-text-messages ("Do not click on any links. Clicking could expose you to scams, download malware, or get your phone number added to lists that are then sold to other bad actors.").

which then automatically requested that she fill in her bank account information, including her password. When she did that, the scammer was able to manipulate the app such that $1500 was withdrawn from her bank account.[42]

There is currently no system to raise a red flag for consumers regarding automated scam texts. As a result, we urge the Commission to prioritize the development of rigorous authentication requirement that would be triggered every time a mass text includes a URL. Such an authentication filter might not be necessary for mass texts sent through a registry that uses CTIA best practices, as participating providers presumably already reject texts that do not meet security protocols.[43] But the filter would stop dangerous texts containing URLs sent by mass texters that are not captured by these voluntary platforms. The Commission should seek input on the privacy implications of all technical applications.

Not every text-based scam involves a clickable URL. Some scams direct consumers to call a phone number, at which point the scammer will attempt to gather personal information to facilitate identity theft,[44] or direct consumers to reply with their one-time password (OTP), to gain access to their account by disrupting multi-factor authentication.[45] The Commission should also explore methods to address these scams.

---

[42] This is a common scam. *See* KrebsOnSecurity, The 'Zelle Fraud' Scam: How it Works, How to Fight Back (Nov. 19, 2021), *available at* https://krebsonsecurity.com/2021/11/the-zelle-fraud-scam-how-it-works-how-to-fight-back/. Typically, the scammer characterizes the app as anti-fraud software used by the bank.

[43] *See* CTIA Best Practices, *supra* note 31.

[44] *See* Office of Minnesota Attorney General, Text Message Phishing – or "Smishing" – Scams, *available at* https://www.ag.state.mn.us/consumer/publications/TextMessagePhishing.asp.

[45] *See* Canadian Bankers Ass'n, Beware of One Time Passcode scams with these tips, *available at* https://cba.ca/one-time-passcode-scams.

V. The Commission should address non-SMS text messages.

The Commission has asked for comment on whether the definition of text messages in the TCPA's Truth in Caller ID subsection should be the basis for the rules it is proposing relating to unwanted and illegal texts.[46] As the FCC has noted, that definition of "text messages"[47] referred to as either SMS (Short Message Service) or MMS (Multimedia Messaging Service), does not cover many of the messages that Americans understand as text messages.[48] In particular, it seems to exclude iMessages sent between iPhones, because these are sent over internet protocols.[49]

More than one billion consumers worldwide use iMessage to send text messages.[50] Within the U.S., 17% of consumers surveyed who have any messenger platform have iMessage.[51] Five times the volume of SMS/MMS messages are sent via non-SMS/MMS platforms like iMessage.[52]

---

[46] Proposed Rule, *supra* note 1, at 61,272 ¶ 5.

[47] 47 U.S.C. § 227(e)(8)(C).

[48] Proposed Rule, *supra* note 1, at 61,273 ¶ 15.

[49] *See* Apple, What is the difference between iMessage and SMS/MMS, *available at* https://support.apple.com/en-us/HT207006; Dan Heyler, AppleToolBox, What is iMessage and how is it different to normal text messages? (last updated Aug. 7, 2020), *available at* https://appletoolbox.com/imessage-basic-guide/#iMessages_use_the_Internet.

[50] Zak Doffman, Forbes, *Bad News Confirmed For 1.3 Billion Apple iMessage Users* (Sept. 10, 2022), *available at* https://www.forbes.com/sites/zakdoffman/2022/09/10/why-apple-iphone-ipad-mac-google-android-and-even-windows-10-users-need-secure-messaging/?sh=7cbb12b17fd4.

[51] Statista, Penetration of leading messenger platforms in the United States as of July 2020, *available at* https://www.statista.com/statistics/294439/messenger-app-share-us-users/.

[52] *See* Federal Commc'ns Comm'n, Consumer Advisory Committee, Report on the State of Text Messaging (Aug. 30, 2022), *available at* https://www.fcc.gov/ecfs/document/1083135018370/1 [hereinafter FCC CAC Report].

Scam texts are sent over these non-SMS/MMS platforms as well.[53] Fraudsters use many messaging platforms to perpetrate their crimes because other criminals peddle tools to make it easier for them to do so, such as by using bots to propagate malware that initiates the fraud for them.[54]

As many consumers do not always distinguish between these platforms, they may not be aware that they are more susceptible to scams using, even widely adopted programs such as iMessage.[55] As such, many consumers would expect that a regulation protecting them from text-based robocalls would include protection from scams sent via iMessage. Given the prevalence of consumer use of non-SMS text messaging services[56] and their vulnerability to scams, we urge the Commission to expand the scope of its inquiry after enacting protections for SMS-based text messages.

VI. Conclusion

We appreciate the opportunity to respond to the Commission's Proposed Rule on eliminating unlawful and annoying robotexts.

---

[53] *See* Lori Gil, iMore, *Don't get scammed by iMessages* (last updated Jan. 17, 2018), *available at* https://www.imore.com/dont-get-scammed-imessages.

[54] *See, e.g.,* Lindsey O'Donnell, *Telegram Bots at Heart of Classiscam Scam-as-a-Service* (Jan. 14, 2021), *available at* https://threatpost.com/telegram-bots-classiscam-scam/163061/ (fake classified ads with malware). *See also* KrebsOnSecurity, The Rise of One-Time Password Interception Bots (Sept. 29, 2021), *available at* https://krebsonsecurity.com/2021/09/the-rise-of-one-time-password-interception-bots/ (stealing user credentials/OTP/MFA).

[55] *See, e.g.*, Apple, What is the difference between iMessage and SMS/MMS, *available at* https://support.apple.com/en-us/HT207006.

[56] *See* FCC CAC Report, *supra* note 52, at 5 ("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. 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 especially among younger Americans." (citations omitted)).

Respectfully submitted, this the 10th day of November 2022, by:

Chris Frascella
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036
frascella@epic.org

Margot Saunders
Senior Counsel
National Consumer Law Center
1001 Connecticut Avenue, NW
Washington, DC 20036
msaunders@nclc.org