FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Targeting and Eliminating Unlawful Text Messages	)	CG Docket No. 21-402
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278

Relating to the
Report and Order and Further Notice of Proposed Rulemaking
Issued March 17, 2023

Comments of

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

May 8, 2023

By:
Margot Saunders
Senior Counsel
msaunders@nclc.org
Carolyn L. Carter
Deputy Director
ccarter@nclc.org
National Consumer Law Center
1001 Connecticut Ave., NW
Washington, D.C. 20036

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

Table of Contents

I. Introduction and Summary. 1

II. The escalation of illegal text messages and calls requires effective action by the Commission. 2

III. The proposals to stop unwanted and illegal calls and texts in the FNPRM and Proposed Rule should be more aggressive. 6

A. The Commission should require providers to block all traffic from an upstream provider that ignores notification of illegal traffic. 6

B. The Commission should establish a set of minimum standards for text message campaign registries. 7

C. The Commission should require carriers to block all unregistered text campaigns containing active hyperlinks. 10

D. The Commission should coordinate with the FTC and other partners to target enforcement actions against web domains that host the sites with malicious URLs spread through illegal text messaging. 12

IV. The Commission should codify the rule that its Do-Not-Call rule applies to text messages. 13

V. The Commission can and should close the "Lead Generator Loophole" through affirmation and enforcement of the existing rules instead of the proposed rule changes 15

A. The proposed additional language 47 C.F.R. § 64.1200(f)(9) would *reduce* consumer protections against unwanted telemarketing calls. 15

B. The current requirements for prior express written consent for prerecorded telemarketing calls already limit consent to a single seller which is essential for ensuring consumers can revoke consent to telemarketers. 17

C. The explicit requirements for prior express invitation or permission for telemarketing calls to lines registered on the DNC Registry currently require a signed, written agreement *between* the consumer and the seller. 19

D. Although the current regulations for express consent and invitation for telemarketing calls are routinely ignored, as the existing regulations provide significant protections the Commission should confirm the explicit requirements of its existing regulations. 21

E. The Commission should reaffirm the current specific requirements for express consent and invitation to receive telemarketing calls. 23

VI. The FCC should issue guidance spelling out the requirements of the federal E-Sign Act when an agreement to receive calls is signed electronically, and when an electronic record is used as the written agreement to receive calls.....23

A. Compliance with the federal E-Sign Act is the only way for electronic signatures and electronic records to legally replace signature and writing requirements.....23

B. For an electronic act to be considered a signature that can provide prior express written consent or prior express invitation or permission, it must meet the requirements for an electronic signature under the E-Sign Act.....25

C. For an electronic record to satisfy a requirement that information be provided to a consumer in writing, the E-Sign Act's consent process must first be followed. ...26

1. The E-Sign Act requires an explicit process before an electronic record can satisfy a writing requirement. 26

2. A consumer must provide E-Sign Act consent before the written agreement required for TCPA consent or permission is presented.....28

3. Oral communications cannot be used to satisfy the FCC's requirement for written agreements for consent and permission. 29

4. The E-Sign Act consent process is not optional. 30

D. The FCC should issue guidance explaining how the E-Sign Act's requirements apply to its regulations. 31

VII. Conclusion. 32

Appendix 34

Comments

I. Introduction and Summary.

The **National Consumer Law Center** (NCLC), on behalf of its low-income clients, and the **Electronic Privacy Information Center**, file these comments along with **Appleseed Foundation, Consumer Action**, **Consumer Federation of America**, **National Association of Consumer Advocates**, **National Association of State Utility Consumer Advocates (NASUCA)**, **National Consumers League**, **Public Citizen**, **Public Knowledge**, and **U.S. PIRG**,[1] regarding the issues raised in the Report and Order and Further Notice of Public Rulemaking (FNPRM) regarding "Targeting and Eliminating Unlawful Text Messages" issued on March 17, 2023.[2] We appreciate the Federal Communication Commission's (Commission or FCC) recognition of the problem of unlawful text messages, and particularly its consideration of ways to reduce the number of unlawful telemarketing texts and calls. While we strongly support several of the Commission's proposals, we urge the Commission to move in a different direction regarding consent to receive telemarketing calls.

As the Commission is aware, the problem of unlawful text messages has escalated in recent years. As we explain in **section II,** *infra,* these unwanted text messages, unless addressed, threaten to undermine yet another communication method in this country.

More particularly, as we explain in **section III**, *infra*, regarding the proposal in paragraphs 1 through 5 of the FCC's Synopsis of its proposal,[3] we support the Commission's proposal to require providers to block all traffic from an upstream provider that ignores a notification of illegal traffic. However, we urge the Commission to take more aggressive action to block unregistered text message campaigns.

---

[1] Descriptions of these national consumer and privacy organizations are provided in the Appendix.

[2] *In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Report and Order and Further Notice of Proposed Rulemaking, CG Docket Nos. 21-402, 02-278 (Rel. Mar. 17, 2023), *available at* https://www.fcc.gov/document/fcc-adopts-its-first-rules-focused-scam-texting-0 [hereinafter FNPRM]. The Proposed Rule was published in the Federal Register at 88 Fed. Reg. 20,800 (Apr. 7, 2023) and is available at https://www.govinfo.gov/content/pkg/FR-2023-04-07/pdf/2023-07069.pdf [hereinafter Proposed Rule].

[3] Proposed Rule, *supra* note 2, at 20,801.

We support the proposal in paragraphs 6 and 7 of the Synopsis to state explicitly that the FCC's Do Not Call (DNC) rule applies to text messages. Even though the existing rule, construed along with court decisions and the Commission's own pronouncements, already makes this conclusion quite clear, it will be helpful to codify this rule explicitly. To avoid unintentionally creating a defense against illegal telemarketing texts that are the subject of pending litigation, the Commission should articulate that this codification is not a change in the law.

In **section V,** *infra***,** we explain why the proposals outlined in paragraphs 8 and 9 of the Synopsis are problematic. While well-intentioned and designed to prevent abuse of the consumer consent process by online lead generators, the proposed rule would represent a reduction of the current protections already included in the Commission's regulations issued pursuant to the Telephone Consumer Protection Act (TCPA).[4]

Section VI, *infra*, explains that the federal E-Sign Act applies when an agreement to receive calls is provided to consumers in an electronic record and the consumer signs it electronically. This means that, to be a valid signature, the electronic action the consumer takes to sign (*e.g.*, by checking a box or typing one's name) must meet the requirements for an electronic signature under the E-Sign Act; and the use of the E-Sign Act's consumer consent process is mandatory when an electronic record is supplied to satisfy a requirement for information to be provided in writing.

II. The escalation of illegal text messages and calls requires effective action by the Commission.

The Commission needs to act forcefully to stop the unrelenting onslaught of illegal calls and unwanted texts to American telephones. The numbers of text-borne scams and the direct losses to consumers resulting from them have escalated dramatically in recent years. In 2018, the FTC reported that consumers lost more than $60 million from text-initiated frauds.[5] By 2021, the consumer-reported losses from text-based frauds surpassed $130 million, and in 2022 the reported losses rose to more than $325 million.[6] That is more than a 400% increase over a four-year period.

---

[4] 47 U.S.C. § 227.

[5] FTC Consumer Sentinel Network, Fraud Reports by Contact Method, Reports & Amount Lost by Contact Method (last visited Apr. 25, 2023) (Losses & Contact Method tab, with quarters 1 through 4 checked for 2018), *available at* https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts.

[6] *Id.* (quarters 1 through 4 checked for years 2021, 2022).

Yet, as the FTC numbers are based solely on reports made by consumers, they represent only a small fraction of the total universe of actual losses from text scams. As indicated by private sector calculations of losses from scam texts, the actual losses to consumers from text-initiated frauds are, undoubtedly, exponentially greater. One survey—Robokiller—reports the number to be closer to $20 billion in annual consumer losses.[7]

In the FNPRM, the Commission estimates direct losses to consumers from scam texts at $2 billion annually,[8] and the inconvenience costs of receiving unwanted spam texts at $6.3 billion annually.[9] We agree with the Commission's characterization of these figures as "conservative," especially given the much higher sums identified through surveys.

Regardless of the exact amount, these losses demand attention, and we urge the Commission in this proceeding to robustly address the sources through which bad actors obtain contact information about consumers. In addition to significant monetary losses, spam calls and texts pose an increased risk to seniors and cognitively impaired individuals who, for example, may miss important calls because the onslaught of spam causes them to be wary of answering their phone.[10] Multiple commenters in this proceeding have already explained to the Commission how the resale of consumer data is a significant factor in spam calls and texts.[11] The harms caused by the data broker industry[12] have recently triggered increasing scrutiny from the Consumer Financial Protection

---

[7] Robokiller, The state of the robotext in 2022, *available at* https://www.robokiller.com/robokiller-2022-phone-scam-report#The-state-of-the-robotext-in-2022 (last visited Apr. 25, 2023).

[8] FNPRM, *supra* note 2, at ¶ 43 ("Further, we assumed that harm from fraudulent spam texts is about 20% of the harm caused by fraudulent robocalls fraud costs.").

[9] *Id.* at ¶ 44.

[10] *See generally* Nicole Egan, *Rage Against the Machine: Reducing Robocall Abuse to Protect At-Risk Consumers*, 17 U. Mass. L. Rev. 211 (2022).

[11] *See, e.g.*, Comment of Richard Presley (Apr. 11, 2023),*available at* https://www.fcc.gov/ecfs/search/search-filings/filing/10411157882365 ("This is exactly why the [lead generation] industry has never followed the rules and nor will it ever police itself…"); Comments of Responsible Enterprises Against Consumer Harassment (R.E.A.C.H.) (Mar. 10, 2023), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/103100550322688 ("…[and t]he endless resale of consent information—often in untrackable fashion—between numerous middlemen (aggregators and brokers) and for an unlimited duration of time. R.E.A.C.H. applauds the Commission's efforts to end these abusive and inappropriate tactics…"); Anonymous Comment, CG Docket Nos. 21-402, 02-278 (Feb. 27, 2023), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/10224111809296 ("It's the aged data companies that are raking in 500% profit reselling the same consumer data 5 or more times to small businesses who don't know any better about the TCPA to begin with.").

[12] *See* Oversight and Investigations Subcommittee Hearing: "Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy" (Apr. 19, 2023) (YouTube presentation), *available at* https://energycommerce.house.gov/events/oversight-and-investigations-subcommittee-hearing-

Bureau, which issued a Request for Information to determine the business model and practices of this industry.[13] As we point out in section V, *infra*, in order to deal with the problems caused by this industry, the Commission should reiterate that agreements providing consents and invitations for calls cannot be sold or transferred, a position the FTC has already articulated.[14]

Telemarketers regularly claim that they have consent for calls based on information provided by data brokers and lead generators.[15] Indeed, some telecommunications providers accused of transmitting illegal telemarketing calls refuse to block them unless pressed; instead, they claim that the tens of thousands of calls they are processing are legal telemarketing calls, even though the calls are based on consents that are clearly flawed.[16] Some telemarketers have even deliberately altered their online consent forms after learning that they were being investigated, in an attempt to deceive regulators and the courts into thinking that their lead forms had always obtained valid consents.[17]

---

who-is-buying-and-selling-your-data-shining-a-light-on-data-brokers. *See also* Opening Statement of Chair Rodgers: "Data Brokers' Days of Surveilling in the Dark Should be Over" (Apr. 19, 2023), *available at* https://energycommerce.house.gov/posts/chair-rodgers-data-brokers-days-of-surveilling-in-the-dark-should-be-over ("Today we explore ways that we have become just dollar signs for data brokers and Big Tech.").

[13] Press Release, Consumer Fin. Prot. Bureau, CFPB Launches Inquiry Into the Business Practices of Data Brokers (Mar. 15, 2023), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-the-business-practices-of-data-brokers/ ("Modern data surveillance practices have allowed companies to hover over our digital lives and monetize our most sensitive data" (quoting CFPB Director Rohit Chopra)); Consumer Fin. Prot. Bureau, Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, Docket No. CFPB-2023-0020 (Mar. 15, 2023), *available at* https://files.consumerfinance.gov/f/documents/cfpb_request-for-information_data-brokers_2023-3.pdf ("Government agencies, technology and privacy experts, financial institutions, consumer advocates, and others have identified numerous consumer harms and abuses related to the operation of data brokers, including significant privacy and security risks, the facilitation of harassment and fraud, the lack of consumer knowledge and consent, and the spread of inaccurate information.").

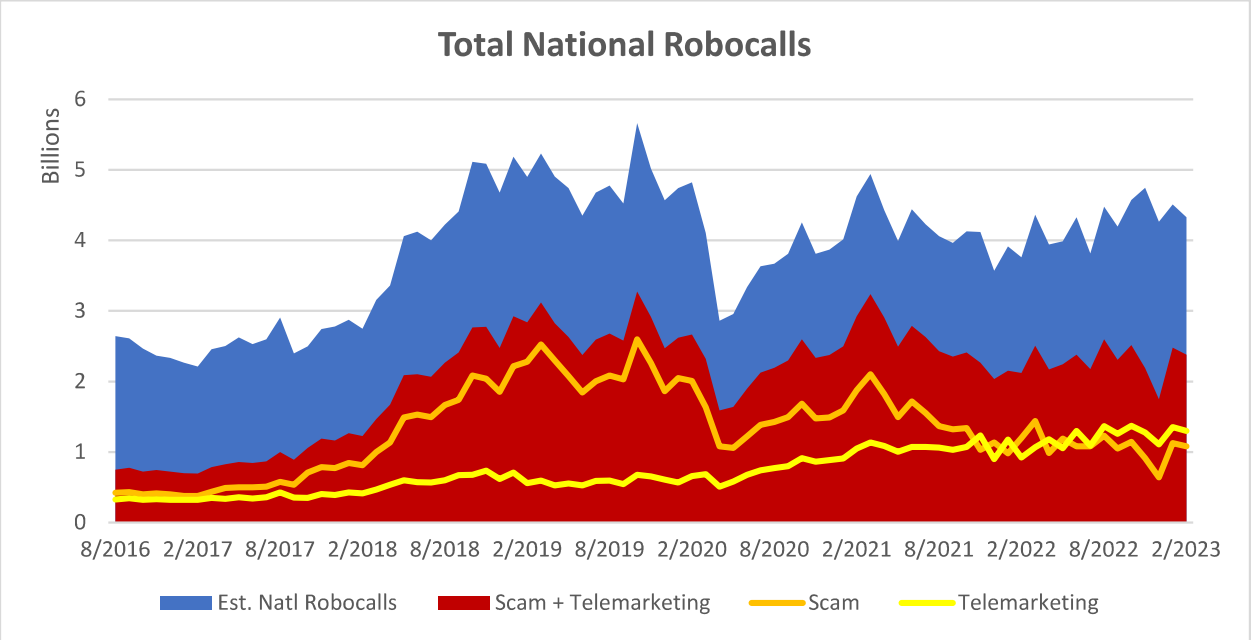
[14] *See* 73 Fed. Reg. 51,163, 51,182 (Aug. 29, 2008).

[15] *See* section V(D), *infra*.

[16] *See, e.g.,* Fed. Commc'ns Comm'n, *In re* Urth Access, Inc., Order, File No. EB-TCD-22-00034232, 2022 WL 17550566, at ¶ 16 (Rel. Dec. 8, 2022), *available at* https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls ("The websites included TCPA consent disclosures whereby the consumer agreed to receive robocalls from 'marketing partners.' These 'marketing partners' would only be visible to the consumer if the consumer clicked on a specific hyperlink to a second website that contained the names of each of 5,329 entities. We find that listing more than 5,000 'marketing partners' on a secondary website is not sufficient to demonstrate that the called parties consented to the calls from any one of these 'marketing partners.'" (footnote omitted) [hereinafter Urth Access Order].

[17] *See* Complaint for Permanent Injunction, Damages, and Other Equitable Relief, State of Ohio *ex rel.* Attorney General Dave Yost v. Jones, No. 2:22-cv-2700, at ¶ 69 (S.D. Ohio July 7, 2022) ("For example, 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

As shown by the red line on the chart below, the number of scam and telemarketing calls per month increased dramatically between 2016 and 2018, and has remained persistently high since then, ranging between 2.5 billion and 3 billion in most months. (The apparent reduction in scam calls and corresponding increase in telemarketing calls is probably a reflection of the third-party provider's reclassification of calls rather than an actual change.[18]).



Telemarketers, sellers, lead generators, and others who benefit from telemarketing calls aggressively and incorrectly interpret current Commission regulations, and completely ignore the requirements of the federal E-Sign Act.[19] Their behavior creates challenges for the enforcement efforts initiated by federal and state authorities, allowing these entities to make claims of plausible deniability. **The Commission has already provided specific regulations governing how sellers and callers must obtain valid consent before telemarketing calls can be made. Yet, the industry has standardized methods for obtaining consent that completely ignore both the**

---

websites in the terms and conditions *after* many VSC robocalls were made based on the alleged 'opt in' from these websites." (emphasis in original)). *See also id.* at ¶¶ 68-71.

[18] YouMail has noted that "calls initially viewed as telemarketing are eventually recognized as illegal telemarketing or scam calls, so it's important to measure the overall quantity of scam and spam calls combined." PR Newswire, Robocalls Top 50.3 Billion in 2022, Matching 2021 Call Volumes Despite Enforcement Efforts (Jan. 5, 2023), *available at* https://www.prnewswire.com/news-releases/robocalls-top-50-3-billion-in-2022--matching-2021-call-volumes-despite-enforcement-efforts-301714297.html.

[19] 15 U.S.C. §§ 7001 *et seq.*; *see* section VI, *infra.*

specific requirements of those regulations and the application of the E-Sign Act to the process. Consumers, well-intentioned sellers, and voice service providers would all benefit from a clear statement of the current requirements for consent for telemarketing calls made with prerecorded messages, and the rules for calls to lines registered on the Do Not Call (DNC) Registry.

For the reasons explained in section V, *infra*, no changes in the current regulations for consent are necessary to deal with the multiple consents supposedly garnered by lead generators. Indeed, the proposals included in the FNPRM would leave consumers with significantly fewer protections than exist through the combination of the current regulations and the proper application of the federal E-Sign Act when consent is obtained through electronic means. The current requirements included in the regulations are more protective of consumers and the integrity of the American telephone system.

III. The proposals to stop unwanted and illegal calls and texts in the FNPRM and Proposed Rule should be more aggressive.

As section II, *supra*, makes clear, the Commission must take action to protect consumers from scammers that are increasingly relying on text messages to defraud Americans. We urge the Commission to implement a system-wide solution to the growing problem of scam texts due to their exponential growth, and not rely on individual enforcement efforts to control these scams. Unless this matter is addressed thoroughly, the trust that the texting platform currently enjoys will be squandered.

We support the Commission's proposal to block all traffic from upstream providers who ignore notification of illegal traffic. We also recommend that the Commission consider whether the following three measures would effectively protect American subscribers from scam and spam texts: 1) creating a set of standards to which text campaign registries must adhere; 2) blocking text messages from campaigns that include active URLs and are not sent through text registries that are in good standing; and 3) working with providers and other agencies (*e.g.* the FTC) as necessary to identify web domains to which malicious URLs direct users.

A. The Commission should require providers to block all traffic from an upstream provider that ignores notification of illegal traffic.

We support the Commission's proposal to require immediate downstream providers to block <u>all</u> traffic from an upstream provider who has failed to block identified suspected illegal

traffic.[20] This is especially important in light of the carrier confusion surrounding the Commission's recent order against Phoneburner,[21] in which Phoneburner believed that downstream providers were directed to block only the illegal traffic, not all traffic, from Phoneburner.[22] A requirement to block only the illegal traffic would create an incentive structure wherein upstream providers could merely offload the responsibility of filtering out illegal traffic to their immediate downstream providers. Requiring that all traffic be blocked creates an effective incentive for the upstream provider to employ more robust measures to protect consumers from unwanted calls and texts, rather than merely pushing the problem downstream.

B. The Commission should establish a set of minimum standards for text message campaign registries.

The Commission has sought comment on how to address text message authentication solutions in light of a mixed record on the issue of spoofing.[23] Carriers have already implemented important safeguards to protect consumers from scam and spam text messages in the form of text message campaign registries. Nevertheless, the statistics reported by the FTC and the private sector underscore the ongoing deficiencies in our current consumer protection regime. As the Commission noted in this rulemaking: "Mobile wireless providers and others have taken steps to protect consumers from potentially harmful text messages; nevertheless, unlawful text messaging is trending in the wrong direction."[24] To change that trendline, the Commission should consider leveraging the existing registry framework by establishing a set of minimum standards for all text registries. At a minimum, the Commission should task text message campaign registries with maintaining records on the sender, the purpose, and the content of every text message campaign submitted for registration.[25]

---

[20] *See* Proposed Rule, *supra* note 2, at ¶ 3.

[21] Federal Commc'ns Comm'n, FCC Warns Providers About Robocalls from PhoneBurner and MV Realty (Jan. 24, 2023), *available at* https://www.fcc.gov/document/fcc-warns-providers-about-robocalls-phoneburner-and-mv-realty.

[22] *See* IsDown, PhoneBurner Status (Jan. 25, 2023), *available at* https://isdown.app/integrations/phoneburner/incidents/170196-service-outage.

[23] *See* FNPRM, *supra* note 2, at ¶ 54.

[24] *Id.* at ¶ 2.

[25] The Commission can look to the FTC's recent TSR rulemaking for suggestions on duration of a record-keeping requirement. *See* 87 Fed. Reg. 33,677, 33,684-33,687, 33,693-33,694 (June 3, 2022), *available at* https://www.federalregister.gov/documents/2022/06/03/2022-09914/telemarketing-sales-rule.

Text message campaign registries, such as the Campaign Registry (which is run by several major wireless service providers and participated in by numerous other industry service providers), facilitate visibility into messaging source and content, as well as establish common standards for text campaigns.[26] SMS senders are incentivized to register their campaigns in exchange for reduced cost and greater reliability in delivery (as registered campaigns do not go through a carrier's filtration process for unregistered, and therefore more suspect, SMS campaigns).[27]

The registration process seems key to eliminating the worst scam texts, as well as limiting the unwanted spam texts. Indeed, the benefits to text campaigns of using registries that abide by CTIA's Messaging Principles and Best Practices[28]—including lower costs for text campaigns and assurance of delivery—makes the registry system a methodology that rewards texters for compliance. But there are no minimum standards for registries. As noted by one industry observer regarding the opaque processes used by different registries: "The problem here is that each carrier or aggregator is operating independently, their rules are not transparent, and they are sometimes slow to react. The biggest issue though is that the carriers do not have visibility into who the end user sending spam messages is."[29] Developing universal standards for text campaign registries would also present an opportunity to address the concerns presented in the record about overbroad and discriminatory blocking and throttling of legal text message campaigns, as well pruning back the thicket of confusing and conflicting requirements among different providers that may serve as barriers to small businesses and non-profit organizations that wish to leverage mass texting for legitimate purposes.[30]

---

[26] The Campaign Registry, https://www.campaignregistry.com/ (last visited Apr. 25, 2023).

[27] Twilio, Help Center, What pricing and fees are associated with the A2P 10DLC service?, *available at* https://support.twilio.com/hc/en-us/articles/1260803965530-What-pricing-and-fees-are-associated-with-the-A2P-10DLC-service (noting different fees for registered and unregistered SMS/MMS messages at AT&T and T-Mobile); Zoom Support, FAQ about 10-Digit Long Code compliance for Zoom Phone and Zoom Contact Center (last updated Mar. 30, 2023), *available at* https://support.zoom.us/hc/en-us/articles/4421899070861-FAQ-about-10-Digit-Long-Code-compliance-for-Zoom-Phone-and-Zoom-Contact-Center (discussing why Zoom customers should register text message campaigns, including issues with filtering and delivery absent registration).

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

[29] Brad Herrmann, Text-Em-All, The Simple Guide to Text Registration (Feb. 24, 2023), *available at* https://www.text-em-all.com/blog/the-simple-guide-to-text-registration.

[30] *See, e.g.*, *In re* Targeting and Eliminating Unlawful Text Messages, Comments of the Coalition for Open Messaging, CG Docket No. 21-402 (Nov. 10, 2022), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/1110088217531.

The CTIA's best practices are effective, clear, and comprehensive. But they are entirely voluntary. Given the escalating numbers of unwanted and illegal texts that include dangerous URLs, we urge the Commission to establish minimum standards for registries that provide texting platforms for texts that include embedded website links. These standards should require the registries to ensure that the texts are legitimate and legal.[31] In particular, the CTIA standards require that embedded website links not obscure the sender's identity and are not intended to harm or deceive the recipient.[32] The best practices outlined in CTIA's Messaging Principles and Best Practices are an excellent basis for the Commission's standards for registries.[33]

The Commission has identified explicitly that one of its goals in this rulemaking is to "help to ensure that all wireless consumers receive the same protections, regardless of which mobile wireless provider they use to receive SMS and MMS messages."[34] It cites to its authority under the TCPA,[35] but also notes that title III and sections 303, 307 and 316 of the Communications Act provide authority to "protect the public from illegal text messages."[36] Requiring all text message campaigns to be held to a minimum standard through a registration process will help ensure that all wireless consumers receive the same protections from scam texts. Finally, if the Commission determines that additional authority would be required to implement these or other strong consumer protections from illegal text messages, it should refresh the record in WT Docket 08-7, and consider

---

[31] CTIA best practices include numerous consumer protections, including requiring consumer consent for A2P texts, requiring express written consent before telemarketing messages, and ensuring that consumers can revoke consent. *See* CTIA Best Practices, *supra* note 28, at § 5.1. Additionally, texters are required to have privacy policies, implement security controls, conduct security audits, and "use reasonable efforts to prevent and combat unwanted or unlawful messaging traffic." *Id.* at § 5.3.1.

[32] *Id.* at § 5.3.2.

[33] *Id.* ("Message Senders should ensure that links to websites embedded within a message do not conceal or obscure the Message Sender's identity and are not intended to cause harm or deceive Consumers. Where a web address (i.e., Uniform Resource Locator (URL)) shortener is used, Message Senders should use a shortener with a web address and IP address(es) dedicated to the exclusive use of the Message Sender. Web addresses contained in messages as well as any websites to which they redirect should unambiguously identify the website owner (i.e., a person or legally registered business entity) and include contact information, such as a postal mailing address.").

[34] FNPRM, *supra* note 2, at ¶ 1.

[35] *Id.* at ¶¶ 38, 65.

[36] *Id.* at ¶ 40.

acting on the pending Petition for Reconsideration of Public Knowledge *et al.* to classify text messaging as a Title II telecommunications service.[37]

C. The Commission should require carriers to block all unregistered text campaigns containing active hyperlinks.

The Commission asks about number spoofing in the context of text messages.[38] As the Commission notes, consumers do not always expect to recognize the sender of a text message, so Caller ID spoofing may not be as relevant in the text context as it is in voice calls.[39] The most serious problem with scam texts is not the number from which the text was sent, but the inclusion of dangerous hyperlinks that allow the texter to access the recipient's personal information or cause other problems. This phenomenon was noted recently by Consumer Reports:

> Delivery scams where fraudsters impersonate Amazon, FedEx, and the U.S. Postal Service are the most prominent text scam, accounting for over 26 percent of all SMS scams in 2021, according to RoboKiller. In these scams, robotexts are sent with links that are purported to be for tracking packages or adjusting user preferences. However, they're actually links that connect users to fake websites where the recipient will divulge their sensitive information or download malware onto their device.[40]

We recommend that the Commission prioritize addressing the unique harm of malicious hyperlinks in application-to-person (A2P) text messages.[41] This is especially important, as current

---

[37] *In re* Petitions for Declaratory Ruling on Regulatory Status of Wireless Messaging Service, Petition for Reconsideration of Public Knowledge et al., WT Docket No. 08-7 (Jan. 28, 2019), *available at* https://www.fcc.gov/ecfs/document/101280325600285/1.

[38] *See* Proposed Rule, *supra* note 2, at ¶ 5.

[39] *See* FNPRM, *supra* note 2, at ¶ 17.

[40] Octavio Blanco, *Smishing: A Silly Word for a Serious Fraud Risk* (updated Sept. 26, 2022), *available at* https://www.consumerreports.org/money/scams-fraud/smishing-a-silly-word-for-a-serious-fraud-risk-a8541743941/(emphasis added).

[41] *See, e.g.*, FNPRM, *supra* note 2, at ¶ 23. *See also* Kaspersky, SMS Attacks and SMS Mobile Threats, *available at* https://www.kaspersky.com/resource-center/threats/sms-attacks (last visited Apr. 25, 2023); Erin McCormick, The Guardian, *Gone in seconds: rising text message scams are draining US bank accounts* (Apr. 22, 2023), *available at* https://www.theguardian.com/money/2023/apr/22/robo-texts-scams-bank-accounts ("When he clicked the link in the text, Koester said it took him to a website with exactly the same design as the USPS homepage."); Dermott Harnett & W. Stuart Jones, Cloudmark Blog, *Freemium free-for-all: How smishing operations take advantage of popular mobile messaging providers* (Nov. 9, 2022), *available at* https://www.cloudmark.com/en/blog/mobile/freemium-free-all-how-smishing-operations-take-advantage-popular-mobile-messaging; Greg Aaron et al., Phishing Landscape 2022: An Annual Study of the Scope and Distribution of Phishing (July 19, 2022), *available at* https://interisle.net/PhishingLandscape2022.pdf; Matti Williamson, Finance Magnates, *Binance Phishing Attack is Underway, Warns CEO Changpeng Zhao* (June 2, 2022),

laws often do not protect consumers from the losses that result after they click on the fraudulent link and provide account information or follow other instructions to transfer funds from their bank accounts to overseas scammers.[42]

We urge the Commission to investigate the possibility of requiring carriers to block A2P messages that contain active hyperlinks that are not registered in the Campaign Registry[43] or another similar registry that meets the minimum standards we recommend in subsection III(B), *supra*. Such an accountability mechanism would both deter bad actor behavior and facilitate investigation of undeterred bad actor behavior.

We recognize that this is a multi-step process: the minimum standards for registries should be established, and registries need time to adopt those standards. Then senders of legitimate text campaigns need to be informed of these new rules. We urge the Commission to inquire of industry commenters and other stakeholders what a reasonable implementation timeframe might be for these requirements and to identify the obstacles that might exist to broader adoption of registration, as well as suggestions for overcoming those obstacles.

We anticipate that industry commenters will argue that the Campaign Registry and others already exist to serve this purpose and carriers do their utmost to protect consumers from scam messages using sophisticated filtering, especially unregistered text campaigns. The fact that reported consumer losses from text-based fraud have increased at least 400% over the past four years is proof that these measures are inadequate. Moreover, text message campaign registration efforts like the Campaign Registry and others are voluntary, inconsistently implemented, and have no penalty for non-compliance, and bad actor campaigns can (and demonstrably have) survived carriers' filtering process for unregistered campaigns.

---

available at https://www.financemagnates.com/cryptocurrency/binance-phishing-attack-is-underway-warns-ceo-changpeng-zhao/.

[42] *See* Comments of National Consumer Law Center, National Community Reinvestment Coalition, and National Consumers League Re: FinCEN-2021-0008, Request for Information Regarding Review of Bank Secrecy Act Regulations and Guidance (Feb. 14, 2022), *available at* https://www.nclc.org/wp-content/uploads/2022/10/FinCEN_AML_comments.pdf. *See also* Erin McCormick, The Guardian, *Gone in seconds: rising text message scams are draining US bank accounts* (Apr. 22, 2023), *available at* https://www.theguardian.com/money/2023/apr/22/robo-texts-scams-bank-accounts ("[A Chase spokesman] said the bank is working to educate customers about scams and has added safeguards such as requiring customers to enter a one-time password sent to their phones before adding new wire transfer payees to their accounts. But, he said, if a customer gives a scammer their passwords or account access, the bank does not reimburse them for the losses.").

[43] The Campaign Registry, https://www.campaignregistry.com/ (last visited Apr. 25, 2023).

If the Commission is committed to protecting consumers from text-based scams, it must develop a regime that will eliminate scam texts that are sent by bad actors who do not register their text message campaigns, while ensuring that this critical communication medium remains open to legitimate users on fair and non-discriminatory terms. As is noted in the report on scam robocalls by NCLC and EPIC, for a method to be effective and sustainable, it must be a systematic, rules-based regime that does not rely on individual enforcement efforts.[44]

D. The Commission should coordinate with the FTC and other partners to target enforcement actions against web domains that host the sites with malicious URLs spread through illegal text messaging.

The Commission should work with its agency partners, such as the Federal Trade Commission (FTC), to develop systemic solutions to identify and shut down the websites that malicious URLs point to. This was a severe problem in 2019,[45] and continues to be a problem today.[46] The FTC recently initiated a rulemaking about these issues specifically in the context of government and business imposters.[47] The FCC should align its policy solutions with the FTC's as they relate to malicious URLs that direct text message subscribers to impersonation websites. As providers identify illegal traffic and malicious URLs, the FCC should develop processes through which providers can deliver information about known bad actors to regulatory and enforcement partners like the FTC on an ongoing basis. As we note *supra*, the Commission should not limit itself to enforcement efforts alone, but rather should explore systemic solutions to address a systemic problem.

---

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

[45] *See* Caitlin Cimpanu, ZDNet, GoDaddy takes down 15,000 subdomains used for online scams (Apr. 25, 2019), *available at* https://www.zdnet.com/article/godaddy-takes-down-15000-subdomains-used-for-online-scams/.

[46] *See* Lawrence Abrams, BleepingComputer, NameCheap's email hacked to send Metamask, DHL phishing emails (Feb. 12, 2023), *available at* https://www.bleepingcomputer.com/news/security/namecheaps-email-hacked-to-send-metamask-dhl-phishing-emails/; Stu Sjouwerman, KnowBe4, Security Awareness Training Blog, *Scammers Still Exploit Hijacked GoDaddy Domains* (Feb. 7, 2023), *available at* https://blog.knowbe4.com/scammers-still-exploit-hijacked-godaddy-domains.

[47] Federal Trade Comm'n, Trade Rule on Impersonation of Government and Businesses, Notice of Proposed Rulemaking; Request for Public Comment, 87 Fed. Reg. 62,741 (Oct. 17, 2022), *available at* https://www.govinfo.gov/content/pkg/FR-2022-10-17/pdf/2022-21289.pdf.

IV. The Commission should codify the rule that its Do-Not-Call rule applies to text messages.

The FCC has repeatedly ruled that the TCPA prohibition against autodialed calls to cell phones "encompasses both voice calls and text calls to wireless numbers including, for example, short message service (SMS) calls."[48] In 2016, the Supreme Court endorsed this view, holding that "[a] text message to a cellular telephone, it is undisputed, qualifies as a 'call' within the compass of § 227(b)(1)(A)(iii)."[49] Decisions from appellate and district courts have likewise held that texts are considered calls for purposes of subsection (b).[50]

The Commission's prior rulings that a text message is a call have been issued in the context of the TCPA's restrictions on autodialed and prerecorded calls to wireless numbers, not its Do Not

---

[48] *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. 14,014 at ¶ 165 (F.C.C. July 3, 2003) ("[U]nder the TCPA, it is unlawful to make *any call* using an automatic telephone dialing system or an artificial or prerecorded message to any wireless telephone number. …This encompasses both voice calls and text calls to wireless numbers including, for example, short message service (SMS) calls…." (emphasis in original)). *Accord In re* Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, Declaratory Ruling, CG Docket No. 02-278, 2023 WL 415622, at ¶ 3 (F.C.C. Jan. 23, 2023) ("The prohibition on using an autodialer to call a wireless number also applies to text messages sent using an autodialer."); *In re* Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, Declaratory Ruling & Order, CG Docket No. 02-278, 2022 WL 17225556, at ¶¶ 6–20 (F.C.C. Nov. 21, 2022) (citing the similarity between text messages and ringless voicemail as a reason to hold that ringless voicemail is subject to the TCPA's protection against autodialed or prerecorded messages to cell phones); *In re* Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, Declaratory Ruling and Order, CG Docket No. 02-278, 30 F.C.C. Rcd. 7961 at ¶¶ 27, 107–108, 111–115 (F.C.C. July 10, 2015) (consent requirement of 47 C.F.R. § 64.1200(a)(1) applies to text messages), *appeal resolved*, ACA Int'l v. Fed. Commc'ns Comm'n, 885 F.3d 687 (D.C. Cir. 2018) (setting aside two parts of 2015 declaratory ruling but leaving this portion undisturbed).

[49] Campbell-Ewald Co. v. Gomez, 577 U.S. 153, 156, 136 S. Ct. 663, 193 L. Ed. 2d 571 (2016). *Accord* Barr v. Am. Ass'n of Political Consultants, Inc., ___ U.S. ___, 140 S. Ct. 2335, 2344 n.1, 207 L. Ed. 2d 784 (2020) (the robocall restriction "bars both automated voice calls and automated text messages").

[50] Duran v. La Boom Disco, Inc., 955 F.3d 279, 280 (2d Cir. 2020), *cert. granted, judgment vacated on other grounds*, 141 S. Ct. 2509 (2021) (remanding for further consideration in light of *Facebook, Inc. v. Duguid*, 141 S. Ct. 1163 (2021), which interpreted definition of autodialer); Warciak v. Subway Restaurants, Inc., 949 F.3d 354, 356 (7th Cir. 2020); Van Patten v. Vertical Fitness Grp., 847 F.3d 1037, 1041–1042 (9th Cir. 2017); Keating v. Peterson's Nelnet, L.L.C., 615 Fed. Appx. 365 (6th Cir. 2015); Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 952 (9th Cir. 2009) ("a text message is a 'call' within the meaning of the TCPA"); Barton v. Temescal Wellness, L.L.C., 525 F. Supp. 3d 195, 198–199 (D. Mass. 2021) (explaining that "[t]he overwhelming weight of precedent holds that text messages are calls for the purposes of the TCPA"); Agbim v. Zip Capital Grp., L.L.C., 2021 WL 4125874 (C.D. Cal. Feb. 2, 2021); Williams v. Myler Disability, L.L.C., 2020 WL 6693134, at *5 (W.D.N.C. Nov. 12, 2020); Griffith v. ContextMedia, Inc., 235 F. Supp. 3d 1032 (N.D. Ill. 2016) (unwanted text messages encroach on consumers' freedom to choose how their telephones are used just as much as unwanted calls do; recipients have Article III standing even though text messaging did not exist when TCPA was passed); Reardon v. Uber Techs., Inc., 115 F. Supp. 3d 1090 (N.D. Cal. 2015).

Call (DNC) rule. But the Commission's rule, 47 C.F.R § 64.1200(e), explicitly applies its DNC regulations to wireless telephone numbers. It would be anomalous to conclude that text messages to wireless numbers are calls for one part of the Commission's TCPA rule but not for the DNC rule. As the DNC rule applies to calls to wireless numbers, and text messages to wireless numbers are calls for purposes of other parts of the rule, text messages must also be calls for purposes of the DNC rule. Many courts have so held.[51]

The general treatment of text messages as calls is confirmed by the 2019 Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. The TRACED Act added a new subsection to the TCPA requiring the FCC to issue regulations to facilitate information-sharing to address unwanted robocalls and spoofed calls. The new subsection explicitly extends to both calls and text messages sent in violation of the statute:

> Sec. 10. Stop Robocalls.
>
> (a) Information Sharing Regarding Robocall and Spoofing Violations.—Section 227 of the Communications Act of 1934 (47 U.S.C. 227) is amended by adding at the end the following: (i) Information Sharing.— (1) In general.—Not later than 18 months after the date of the enactment of this subsection, the Commission shall prescribe regulations to establish a process that streamlines the ways in which a private entity may voluntarily share with the Commission information relating to— (A) a call made or a text message sent in violation of subsection (b); . . . [52]

As "subsection (b)" applies only to "calls" (and faxes), text messages can be sent "in violation of subsection (b)" only if they are considered calls. It is clear that Congress continues to treat text messages as calls under the TCPA.

For all these reasons, we strongly support the Commission's proposal to codify the conclusion that text messages are calls for purposes of the DNC rule and the TCPA's other

---

[51] *See, e.g.,* Pariseau v. Built USA, L.L.C., 619 F. Supp. 3d 1203 (M.D. Fla. 2022) (text message is a call for purposes of do-not-call rule); Gill v. Align Tech., 2022 WL 1540016, at *3–4 (E.D. Wis. May 16, 2022) (failing to honor do-not-call request within reasonable time is a violation; refusing to dismiss claim that texting and calling plaintiff a few hours after her do-not-call request was a violation); Visco v. Creditors Relief, L.L.C., 2022 WL 488495 (D. Mass. Feb. 17, 2022); Barton v. Temescal Wellness, L.L.C., 525 F. Supp. 3d 195 (D. Mass. 2021) (text message touting sellers' extended hours and including a link to its "menu" of goods and services is a solicitation); Mantha v. Quotewizard.com, L.L.C., 2021 WL 6061919, at *7 (D. Mass. Dec. 13, 2021) (text message offering an insurance quote is a telephone solicitation, as its purpose is to encourage the purchase of a service), *adopted*, 2022 WL 325722, at *7 (D. Mass. Feb. 3, 2022); Sagar v. Kelly Auto. Grp., Inc., 2021 WL 5567408 (D. Mass. Nov. 29, 2021) (text message is a call for purpose of do-not-call rule). *See generally* National Consumer Law Center, Federal Deception Law § 6.7.2.2 (4th ed. 2022).

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

prohibitions. To ensure that this action does not undermine any claims for violations of the rules, the Commission should state that the codification is not a change in the law.

V. The Commission can and should close the "Lead Generator Loophole" through affirmation and enforcement of the existing rules instead of the proposed rule changes.

We strongly support the Commission's decision to take action against the practices of lead generators and data brokers to develop illegal mass "consent" shields for telemarketing calls. However, the Commission's proposed approach of revising 47 C.F.R. § 64.1200(f)(9) is unnecessary, will undermine key consumer protections in the current regulations, and will introduce conflicts and ambiguities in other areas. As explained further below, the current requirements for prior express written consent or permission for telemarketing calls limit consent to a single seller and provide more protections against telemarketing calls than the new proposed language. While the Commission's proposed rule clearly aims to balance consumer convenience and consumer protection, the proposed changes will introduce more complexity and uncertainty into an already complex regime, and undermine the ultimate consumer protection goal.

The Commission should simply affirm the single seller interpretation of § 64.1200(f)(9) and be prepared to take enforcement action against telemarketers making use of illegitimately obtained consumer "consent."

A. The proposed additional language 47 C.F.R. § 64.1200(f)(9) would *reduce* consumer protections against unwanted telemarketing calls.[53]

In the Proposed Rule Synopsis paragraphs 8 and 9, the Commission proposes to "ban the practice of obtaining a single consumer consent as grounds for delivering calls and text messages from multiple marketers on subjects beyond the scope of the original consent."[54] We applaud the Commission's goal of reining in the widespread abuses created by lead generators, bots, and data brokers.

However, as described in **subsection V(B),** *infra*, the current regulation for prior express consent at 47 C.F.R. § 64.1200(f)(9) for prerecorded telemarketing calls to residential lines *already*

[53] To simplify terminology in these comments, we speak generally about "calls," which the Commission has clearly stated include texts. *See* section IV(A), *supra.*

[54] Proposed Rule, *supra* note 2, at ¶ 8.

bans this practice. In fact, the current rule is more protective of consumers because it limits the consumer's agreement to calls from a single seller. An important benefit of the one-seller approach in the current regulation is that it ensures that consumers can revoke consent for calls from those sellers. As explained in subsection V(B), *infra*, the Commission's proposal, which would allow a consumer's agreement to receive calls to apply to multiple sellers, would impair the consumer's ability to revoke consent. We oppose the FCC's proposed revision to subsection (f)(9) because it would cut back on these protections.

Another reason that we oppose the FCC's proposed revision is that it would make subsection (f)(9) inconsistent with the Commission's current requirements for agreements that provide prior express invitation or permission for telemarketing calls to lines registered on the Do Not Call Registry (DNC) at 47 C.F.R. § 64.1200(c)(2)(ii)**.** As we explain in **subsection (V)C**, *infra*, that rule also limits consent to a single seller because it explicitly requires that the agreement be *between* the consumer and the seller**.** Since telemarketing calls that are prerecorded and calls that are made to lines registered as DNC lines are required to comply with both sets of applicable requirements—those for prerecorded telemarketing calls at 47 C.F.R. § 64.1200(f)(9), as well as those for calls to DNC lines—the new language would potentially undermine the current protections for calls to DNC lines and create conflicts that do not now exist.

Subsection V(D), *infra*, explains how the current regulations for consent and permission for telemarketing calls are routinely ignored, even though the specific requirements of the existing regulations provide significant protections against unwanted telemarketing calls.

In **subsection V(E),** *infra*, we outline the guidance that we ask the FCC to issue to facilitate future compliance, which we believe should drastically reduce the incidence of unwanted and illegal telemarketing calls—at least from those telemarketers that strive to comply with the law.

Section VI, *infra*, explains the interaction between the E-Sign Act and the Commission's current regulations for written agreements that provide consent or invitation for telemarketing calls. As most agreements for consent or invitation to allow telemarketing calls are entered into through electronic media (either online or—purportedly—over the telephone), the federal E-Sign Act's requirements for electronic signatures, and for delivery of writings to consumers through electronic records, are implicated. As explained, when an electronic record is signed with an electronic signature, the signature must be attached to or logically associated with the agreement signed. As a result, the E-Sign Act, as applied to the current regulations, provides further assurance that a party

cannot legally sign multiple agreements providing for prior express written consent with one electronic click.

B. The current requirements for prior express written consent for prerecorded telemarketing calls already limit consent to a single seller which is essential for ensuring consumers can revoke consent to telemarketers.

The FCC's current rules allow telemarketing calls that use prerecorded or artificial voice messages ("prerecorded calls") to residential lines only if the called party has provided prior express written consent,[55] which the current regulations define as—

> (9) The term prior express written consent means an agreement, in writing, bearing the signature of the person called that clearly authorizes the seller to deliver or cause to be delivered to the person called advertisements or telemarketing messages using an automatic telephone dialing system or an artificial or prerecorded voice, and the telephone number to which the signatory authorizes such advertisements or telemarketing messages to be delivered.
>
> (i) The written agreement shall include a clear and conspicuous disclosure informing the person signing that:
>
> (A) By executing the agreement, such person authorizes the seller to deliver or cause to be delivered to the signatory telemarketing calls using an automatic telephone dialing system or an artificial or prerecorded voice; and
>
> (B) The person is not required to sign the agreement (directly or indirectly), or agree to enter into such an agreement as a condition of purchasing any property, goods, or services.
>
> (ii) The term "signature" shall include an electronic or digital form of signature, to the extent that such form of signature is recognized as a valid signature under applicable federal law or state contract law.[56]

By referring twice to "the seller," this definition makes it clear that the consent form can only authorize calls from a single specifically named seller and cannot authorize calls made by or on behalf of any other entity. The regulations define the word "seller" to mean "*the* person or entity on whose behalf a telephone call or message is initiated for the purpose of encouraging the purchase . . . of goods or services."[57] By contrast, the term "telemarketer" is defined by subsection (f)(12) as the

---

[55] 47 C.F.R. § 64.1200(a)(3).

[56] 47 C.F.R. § 64.100(f)(9) (emphasis added).

[57] 47 C.F.R. § 64.100(f)(10) (emphasis added).

person that "initiates a telephone call . . .."

Despite the specific words in the current version of 47 C.F.R. § 64.1200(f)(9) regarding how prior express written consent can be obtained, the telemarketing industry routinely ignores its requirements, as explained in section V(D), *infra*. The new language proposed in the Proposed Rule would permit one consent agreement to authorize multiple telemarketers to call, each offering sales from different sellers, which is not permitted under the current regulations.

If one agreement could provide the basis for calls from multiple sellers, it would be impossible for the recipient of the calls to revoke consent for calls from those multiple sellers. Yet, as the Commission noted,[58] the ability of call recipients to revoke prior express consent is a critically important way for consumers to control and limit these calls. Both the FCC and the FTC impose multiple requirements to ensure that recipients of telemarketing calls can revoke any prior consent to be called. All prerecorded voice telemarketing calls must include an automated opt-out mechanism in each call.[59] Telemarketing callers are required to identify both the name of the caller and the seller, and provide "a telephone number or address" to contact the caller or seller.[60] Finally, all telemarketing callers—including those making prerecorded calls to residential lines and live calls to persons on the DNC Registry—must maintain a list of persons who do not wish to be called, and must comply with such requests.[61]

The combined requirements in the current regulations that a) limit the agreements for consent permit calls from only one seller at a time, and b) require that each prerecorded telemarketing call includes an easy method for the recipient to revoke consent to each caller, represent the Commission's prior recognition of the importance of ensuring that consent must always be effectively revocable. Consent, as a noun, is "compliance in or approval of what is done or proposed by another," and the action of consent is "to give assent or approval."[62] Compliance or approval can be withdrawn at any point while the act of giving approval can similarly be changed;

---

[58] *See In re* Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, Report and Order, CG Docket No. 02-278, 27 F.C.C. Rcd. 1830, at ¶ 48 (F.C.C. Feb. 15, 2012) [hereinafter 2012 Report and Order]. *See also id.* at 1875 (Statement of Chairman Julius Genachowski).

[59] 47 C.F.R. § 64.1200(b)(3); 16 C.F.R. § 310.4(b)(v)(B)(ii)(B). And messages left on voicemail must include opt-out instructions. *Id.*

[60] 47 C.F.R. § 64.1200(d)(4); 16 C.F.R. § 310.4(b)(v)(B)(ii)(B).

[61] 47 C.F.R. § 64.1200(d)(3); 16 C.F.R. §§ 310.4(b)(1)(ii) & (iii).

[62] Merriam-Webster Dictionary (11th ed. 2022).

consent therefore cannot be truly guaranteed if it is not revocable. The FCC's 2015 Declaratory Ruling, upheld by the D.C. Circuit,[63] emphasizes the importance of revocation of consent, and makes clear that any statement in which "the called party clearly express[es] his or her desire not to receive further calls" is sufficient to show revocation.[64] However, if one agreement could permit multiple callers to make calls—as would be the case should the proposed amendment to 47 C.F.R. § 64.1200(f)(9) be promulgated—revoking consent during a call from one seller would not revoke consent from the other sellers or telemarketers whose names were included in the agreement. This would expose subscribers to many more telemarketing calls than would the enforcement of the current regulations and would significantly undermine their ability to revoke consent to calls and texts.

As the proposed new language to be added to the end of the 47 C.F.R. § 64.1200(f)(9) would undermine the current protections by expressly permitting the continuation of the illegal practices currently used by the telemarketing industry, we urge the Commission not to promulgate the proposed language. Instead, it should retain the current language, and issue a clear statement that the language means that agreement providing prior express written consent can only relate to calls from just one seller.

C. The explicit requirements for prior express invitation or permission for telemarketing calls to lines registered on the DNC Registry currently require a signed, written agreement *between* the consumer and the seller.

Telemarketing calls and texts to residential lines that are subscribed to the DNC Registry are prohibited unless the recipient has provided prior express invitation or permission, the caller has an established business relationship with the called party, or the call is by or on behalf of a tax-exempt organization.[65] A telemarketing call made to a DNC-registered line that also includes a prerecorded

---

[63] *In re* Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, Declaratory Ruling and Order, CG Docket No. 02-278, 30 F.C.C. Rcd. 7961 at ¶¶ 55, 56, 57; ACA Int'l v. Fed. Commc'ns Comm'n, 885 F.3d 687 (D.C. Cir. 2018).

[64] *In re* Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, Declaratory Ruling and Order, CG Docket No. 02-278, 30 F.C.C. Rcd. 7961 at ¶ 67 (F.C.C. July 10, 2015), *ruling upheld*, ACA Int'l v. Fed. Commc'ns Comm'n, 885 F.3d 687 (D.C. Cir. 2018) (upholding this portion of 2015 Declaratory Ruling).

[65] 47 C.F.R. § 64.1200(f)(15) (definition of "telephone solicitation").

message must comply with both the rules for prerecorded calls and the rules for calls to DNC lines.[66]

To obtain prior express invitation or permission for a telemarketing call to a DNC line, the caller must meet the requirements of 47 C.F.R. § 64.1200(c)(2)(ii):

> 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 and includes the telephone number to which the calls may be placed;[67]

This consent process is similar to that required for prerecorded telemarketing calls, discussed in section V(B), *supra*. It requires that the recipient sign a written agreement that includes the required statement that the consumer "agrees to be contacted by this seller." The reference to "this seller" makes it particularly clear that each agreement can relate to only one particular seller.

In addition, this regulation goes beyond the consent process for prerecorded telemarketing calls, which can be obtained by a third party, in that it requires that the agreement evidencing prior express invitation for calls to lines on the DNC Registry be *between* the seller and the consumer. The plain language of the regulation means that, unless it is the seller's agent acting on behalf of the seller, neither a telemarketer nor a lead generator can broker the agreement providing express permission to make a telemarketing call to a line subscribed on the DNC Registry. Only the seller can enter into an agreement with a consumer to allow telemarketing calls to that consumer's line if it is registered on the DNC Registry.

Maintaining the current requirement for an agreement providing prior express consent or invitation to one seller at a time would still permit called parties to go to a lead generator's website and check multiple boxes in serial fashion, allowing consumers to apply a separate checkmark to a box that indicates their intent to consent to be called by the seller whose agreement is included next to each box. However, the seller, rather than the telemarketer or the lead generator, must be party to the agreement.

---

[66] Among other things, this means that there is no exception based on an established business relationship for prerecorded telemarketing calls to DNC lines. *See* 2012 Report and Order, *supra* note 58, at ¶ 48.

[67] 47 C.F.R. § 64.1200(c)(2)(ii) (emphasis added).

D. Although the current regulations for express consent and invitation for telemarketing calls are routinely ignored, as the existing regulations provide significant protections the Commission should confirm the explicit requirements of its existing regulations.

As noted above, the Commission should not adopt its proposed addition to the definition of prior express written consent, as the proposed addition would reduce current protections against unwanted calls. Instead, the Commission should issue a declaratory ruling providing guidance about compliance with the current regulation, as set out in section V(E), *infra*. This guidance is necessary because the explicit requirements for both types of consent are routinely ignored by callers and telemarketers.[68] Making it clear that the rules for prior express written consent and prior express invitation or permission mean what they say would go a long way toward deterring callers' widespread abuse and misuse of the consent process, including preventing lead generators from purporting to obtain consent for multiple entities—typically hidden behind a hyperlink—to make telemarketing calls.[69] The current regulations already set forth the bright-line limits of one seller for each agreement providing consent or permission for telemarketing calls. This would address much of the harm outlined in section II, *supra*, by locking down fraudulent attempts to claim consent, as well as pretextual arguments where no attempt to obtain consent was ever made (for example, where the telemarketer simply purchased a list of consumer information).

Enforcing the one-seller requirement would mean that consumers who agree to receive calls from a particular seller will have provided true and meaningful consent for calls from an identified seller from whom they want to hear. It will also make purported consent more easily verifiable. Instead of having to reconstruct a website that may or may not have included a particular seller in a hyperlinked list,[70] there will either be a signed agreement with the seller that names the seller on

---

[68] *See, e.g.,* Urth Access Order, *supra* note 16 ("The websites included TCPA consent disclosures whereby the consumer agreed to receive robocalls from 'marketing partners.' These 'marketing partners' would only be visible to the consumer if the consumer clicked on a specific hyperlink to a second website that contained the names of each of 5,329 entities. We find that listing more than 5,000 'marketing partners' on a secondary website is not sufficient to demonstrate that the called parties consented to the calls from any one of these 'marketing partners.'" (footnote omitted)).

[69] *Id.* Indeed, in this case, the defendants changed the language on their lead form after the Ohio Attorney General filed the case against them to try and retroactively make it appear that the consent was clear and conspicuous.

[70] *See, e.g.*, Williams v. Pillpack L.L.C., 2021 WL 535215, at *6 (W.D. Wash. Feb. 12, 2021) (certifying class; noting that the seller had not even "presented evidence that the website opt-in forms listed Prospects DM (or one of its fictitious names) as a Marketing Partner *before* the Class members were called" (emphasis in original)).

whose behalf the calls were made or there will not.

Enforcing the existing consent requirements as written will also likely cut down on the current widespread fraud and falsification of consent.[71] It will mean that sellers will be expected to have evidence of specific agreements with consumers to receive calls. Sellers will need to know the source of these consents. They will not be able to accept purported leads that were generated by a chain of contractors and subcontractors, and they will not be able to argue that they were unaware of any illegal activities.

Moreover, as the current FCC regulation explicitly requires that the agreements for both consent for prerecorded calls and express permission for calls to DNC lines must name the specific seller for whose calls the consumer is agreeing to receive, these agreements should not be transferable between sellers. A consumer who consents to receive calls from Seller A has not consented to receive calls from Seller B. The FCC's guidance should reinforce this rule.

Issuing guidance to enforce both the one-seller rule and non-transferability would also ensure that the FCC's rule remains consistent with that of the FTC. The FTC has stated that its Telemarketing Sales Rule requires that each seller have its own agreement for calls with the consumer receiving the calls, and that consents cannot be transferred between telemarketers and sellers:

> [T]he Commission emphasizes that a consumer's agreement with a seller to receive calls delivering prerecorded messages is nontransferable. Any party other than that particular seller must negotiate its own agreement with the consumer to accept calls delivering prerecorded messages. Prerecorded calls placed to a consumer on the National Do Not Call Registry by some third party that does not have its own agreement with the consumer would violate the TSR. . . . [72]

---

[71] *See, e.g.*, McCurley v. Royal Seas Cruises, Inc., 2022 WL 1012471, at *2, 3 (9th Cir. Apr. 5, 2022) (noting the many discrepancies in a lead generator's records of purported consent; defendant's claim re level of consent is "implausible at best"); Mantha v. Quotewizard.com, L.L.C., 2021 WL 6061919, at *9 (D. Mass. Dec. 13, 2021) (Mag.) (granting partial summary judgment to plaintiff on issue of consent to receive calls despite being on nationwide do-not-call list; observing that lead generator apparently pirated another company's website in order to generate or falsify the source of leads, one of which resulted in the call to plaintiff), *adopted*, 2022 WL 325722 (D. Mass. Feb. 3, 2022). *See also* HI.Q, Inc. v. ZeetoGroup, L.L.C., 2022 WL 17345784 (S.D. Cal. Nov. 29, 2022) (Mag.) (describing background before granting regarding motion to compel; lead generator submitted three sworn statements, one saying that consent form identified caller and two saying it did not, and some of its "validation reports" were links that did not work).

[72] 73 Fed. Reg. 51,163, 51,182 (Aug. 29, 2008) (emphasis added).

In the Do-Not-Call Implementation Act, Congress specifically required the FCC to coordinate its do-not-call rule with the FTC and maximize consistency between the two rules.[73] It is incumbent on the FCC to articulate the same interpretation for its own regulations requiring consent for prerecorded telemarketing calls.

E. The Commission should reaffirm the current specific requirements for express consent and invitation to receive telemarketing calls.

For the reasons set forth in section V(A) through (D), *supra*, we ask the Commission to reaffirm and provide more detailed guidance regarding the explicit requirements for prior express written consent to receive prerecorded telemarketing calls made to cellular and residential lines set out in 47 C.F.R. § 64.1200(f)(9), and for prior express invitation or permission to receive telemarketing calls to lines registered on the DNC Registry set out in 47 C.F.R. § 64.1200(c)(2)(ii). Specifically, the Commission should reiterate that:

1. An agreement to receive prerecorded telemarketing calls can authorize such calls for just one specific seller.
2. An agreement to receive calls to a DNC line must be *between* the consumer and the seller.
3. Agreements providing consent or permission cannot be sold or transferred.

VI. The FCC should issue guidance spelling out the requirements of the federal E-Sign Act when an agreement to receive calls is signed electronically, and when an electronic record is used as the written agreement to receive calls.

A. Compliance with the federal E-Sign Act is the only way for electronic signatures and electronic records to legally replace signature and writing requirements.

The federal Electronic Signatures in Global and National Commerce Act (the E-Sign Act) establishes the rules for satisfying a requirement for a writing or a signature with their electronic equivalents.[74] Virtually every state has adopted a similar law, the Uniform Electronic Transactions Act (UETA),[75] but the E-Sign Act alone applies to federal laws and regulations such as the FCC's

---

[73] The Do-Not-Call Implementation Act, Pub. L. No. 108-10, 117 Stat. 557 § 3 (2003).

[74] 15 U.S.C. §§ 7001 *et seq.*

[75] Uniform Elec. Transactions Act, Prefatory Note, at 2, *available at* https://www.uniformlaws.org/viewdocument/final-act-21?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034&tab=librarydocuments ("Whether a record is attributed to a person is left to law outside this Act. Whether an electronic signature has any effect is left to the surrounding circumstances and other law.").

TCPA regulations. The E-Sign Act establishes important limits and protections when electronic records are used in place of writings and electronic signatures are used to satisfy signature requirements. Other federal agencies have recognized that compliance with the E-Sign Act governs this conversion process.[76]

It is because of the E-Sign Act that an electronic action can carry the same legal significance as a "wet" signature. The E-Sign Act provides that "a contract … may not be denied legal effect, validity, or enforceability solely because an *electronic signature* or electronic record was used in its formation."[77] This provision allows an agreement to receive telemarketing calls that is signed with an electronic action to have the same legal significance as if a handwritten signature were applied. But, as discussed in section VI(B), *infra*, in order for the electronic act meant to be a signature can be considered a signature, it must meet the definition for an electronic signature set forth in the E-Sign Act.

An equally important E-Sign Act requirement, found at 15 U.S.C. § 7001(c), applies when an electronic record is used to satisfy a requirement for information to be provided in writing to a consumer. This section of the E-Sign Act requires special rules to ensure that consumers who forgo a written document understand that they are doing so, give true consent, and have the ability to access the information electronically.[78] This separate requirement is discussed in section VI(C), *infra*.

---

[76] *See, e.g.* Consumer Financial Protection Bureau: § 1024.3 E-Sign applicability ("The disclosures required by this part may be provided in electronic form, subject to compliance with the consumer consent and other applicable provisions of the Electronic Signatures in Global and National Commerce Act (E-Sign Act) (15 U.S.C. 7001 *et seq.*)."); National Credit Union Administration: E-Sign Overview ("The Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001 *et seq.*, (E-Sign Act), signed into law June 30, 2000, provides a general rule of validity for electronic records and signatures for transactions in or affecting interstate or foreign commerce. The E-Sign Act allows the use of electronic records to satisfy any statute, regulation, or rule of law requiring that such information be provided in writing, if the consumer has affirmatively consented to such use and has not withdrawn such consent."), *available at* https://ncua.gov/regulation-supervision/manuals-guides/federal-consumer-financial-protection-guide/compliance-management/deposit-regulations/electronic-signatures-global-and-national-commerce-act-e-sign-act; Farm Credit Administration: 12 C.F.R. § 609.910 ("E-SIGN makes it easier to conduct E-commerce. With some exceptions, E-SIGN permits the use and establishes the legal validity of electronic contracts, electronic signatures, and records maintained in electronic rather than paper form. It governs transactions relating to the conduct of business, consumer, or commercial affairs between two or more persons. E-commerce is optional; all parties to a transaction must agree before it can be used.").

[77] 15 U.S.C. § 7001(a)(2) (emphasis added).

[78] 15 U.S.C. § 7001(c). *See* Mantha v. Quotewizard.com, L.L.C., 2021 WL 6061919 (D. Mass. Dec. 13, 2021) (Mag.) (rejecting defendant's claim that plaintiff gave prior express invitation or permission, because of failure to comply with E-Sign Act), *adopted*, 2022 WL 325722 (D. Mass. Feb. 3, 2022).

Section VI(D), *infra*, outlines the guidance the Commission should issue delineating the application of the mandates of the federal E-Sign Act to the TCPA's requirements for consent for prerecorded telemarketing calls and permission for calls to lines registered on the DNC Registry.

B. For an electronic act to be considered a signature that can provide prior express written consent or prior express invitation or permission, it must meet the requirements for an electronic signature under the E-Sign Act.

The FCC's rules for both prior express written consent and prior express invitation or permission require the consumer's signature on a written agreement to receive telemarketing calls. As noted in the preceding section, the E-Sign Act allows an "electronic signature" to replace a written signature.[79] It defines "electronic signature" as:

> [A]n electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.[80]

This definition includes several distinct features: (1) the signature must be an electronic sound, symbol, or process; (2) the sound, symbol or process that constitutes the electronic signature must be attached to or logically associated with the relevant record; and (3) the signature must have been executed or adopted by a person with the intent to sign the record.

The first of these requirements—the "sound, symbol, or process"—could be a click on a checkbox, typing one's name, or writing one's name with a finger or a stylus. The second requirement—that the electronic record be "attached to or logically associated with" the electronic record to be signed—requires that the signature and record signed must be either close in proximity or "logically associated" with each other.

As for the third requirement, an electronic sound, symbol, or process does not in and of itself demonstrate that the consumer took that electronic action with the intent to sign the agreement. When the agreement is to provide consent for telemarketing calls, the place on the electronic form where the electronic action is to be applied must clearly indicate that the consumer, by taking the electronic action, is intending to sign the related electronic agreement to receive those calls. (And, even then, this conclusion is not irrebuttable, given the widespread fraud and falsification of consent forms.)

---

[79] 15 U.S.C. § 7001(a)(2).

[80] 15 U.S.C. § 7006(5); Unif. Elec. Transactions Act § 2(8).

An electronic sound, symbol, or process on a website that is hyperlinked to a list of multiple other parties from whom the person is purportedly agreeing to receive calls would not comply with either the second or third requirements. The electronic action meant to be a signature would not be attached to or logically associated with the names of the telemarketers listed in a hyperlink that is visible only if the consumer hovers the mouse over the relevant hyperlinked word or navigates to a different webpage that contains the list.[81] In addition, the person applying the click likely would not have had the required intent to sign an agreement with all of the callers included in the hyperlinked list.[82] As the Commission noted in its enforcement action against Urth Access, consent purportedly provided to many of potential telemarketing callers at the same time because of a hyperlink on a portion of the consent form is not clear and conspicuous.[83]

Additionally, as courts have noted, a checkbox accompanied by a statement providing consent to receive marketing messages that was automatically filled in with a checkmark by default when a webpage was loaded will not demonstrate the consumer's affirmative consent.[84] For a click to be considered an electronic signature, the signer must affirmatively apply it to the electronic record.

C. For an electronic record to satisfy a requirement that information be provided to a consumer in writing, the E-Sign Act's consent process must first be followed.

1. The E-Sign Act requires an explicit process before an electronic record can satisfy a writing requirement.

In addition to its requirements regarding signatures discussed in the preceding section, the E-Sign Act mandates that a special consent process[85] be followed before a requirement that a

---

81 15 U.S.C. § 7006(5); Unif. Elec. Transactions Act § 2(8).

82 *See* Urth Access Order, *supra* note 16 ("The websites included TCPA consent disclosures whereby the consumer agreed to receive robocalls from 'marketing partners.' These 'marketing partners' would only be visible to the consumer if the consumer clicked on a specific hyperlink to a second website that contained the names of each of 5,329 entities. We find that listing more than 5,000 'marketing partners' on a secondary website is not sufficient to demonstrate that the called parties consented to the calls from any one of these 'marketing partners.'" (footnote omitted)).

83 *Id. See also* 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.

84 *See* Snyder v. icard Gift Card, L.L.C., 2016 WL 7507994, at *6 (S.D. Fla. May 16, 2016).

85 *See* National Consumer Law Center, Consumer Banking and Payments Law § 11.4 (6th ed. 2018), *updated at*

written disclosure be provided to a consumer can be satisfied by the delivery of an electronic record.[86] The Act states that if a statute, regulation, or rule of law requires information to be provided to a consumer in writing, an electronic record can be utilized only if certain conditions are met.[87] First, the consumer must affirmatively consent to such use and must not have withdrawn that consent.[88]

Second, as required by 15 U.S.C. § 7001(c)(1)(C), the consumer, prior to consenting, must be given a clear and conspicuous statement providing information relating to the delivery of electronic records.

Third, and most importantly, for the consumer's consent to receive an electronic record of a written disclosure to be valid, the consumer must consent "electronically . . . in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent."[89] This requirement is a critical test of the validity of the consent to receive the electronic version of the writing. Consumers must demonstrate—not just affirm—that they have access to the equipment and programs necessary to receive, open, and read the relevant electronic documents.[90]

As the legislative history to the E-Sign Act states:

> It means the consumer, in response to an electronic vendor enquiry, actually opens an attached document sent electronically by the vendor and confirms that ability in an e-mail response. . . . It is not sufficient for the consumer merely to tell the vendor in an e-mail that he or she can access the information in the specified formats.[91]

This special consent process is required if a consumer gives prior express written consent or prior express invitation or permission to receive calls electronically because the Commission's rules on both topics require information to be provided to the consumer in writing. In the case of prior express invitation or permission, section 64.1200(c)(2)(ii) requires that the written agreement must

---

www.nclc.org/library (more information on E-Sign consent requirements).

[86] 15 U.S.C. § 7001(c).

[87] 15 U.S.C. § 7001(c)(1).

[88] 15 U.S.C. § 7001(c)(1)(A).

[89] 15 U.S.C. § 7001(c)(1)(C)(ii).

[90] *See* 146 Cong. Rec. S5216 (June 15, 2000) (statement of Sen. Wyden) ("'Reasonably demonstrates' means just that. It means the consumer can prove his or her ability to access the electronic information that will be provided.").

[91] *Id.*

state that the consumer agrees to be contacted by the seller in question, and that the phone number to which calls may be placed must be identified, and this written agreement with these items of information must be given to the consumer for signature. In the case of prior express written consent, section 64.1200(f)(9) is similar, but the disclosure must also inform the consumer that signing the agreement is not a condition of purchasing property, goods, or services. Both of these requirements to provide information to the consumer in writing trigger E-Sign's special consent process if the agreement is provided electronically.

2. A consumer must provide E-Sign Act consent before the written agreement required for TCPA consent or permission is presented.

In order for the electronic delivery of a record to satisfy a requirement that it be in writing, the consumer must first step through the E-Sign Act process to demonstrate consent to receive the information electronically, as specified at 15 U.S.C. § 7001(c)(3). In the typical online solicitation for consent to receive telemarketing calls, the written disclosures required by the TCPA regulations are provided on a website. The E-Sign Act consent disclosures can be provided on the same website and in the same format, but the E-Sign Act requires the consumer to step through the E-Sign process before being provided the electronic record containing the required written agreement to receive telemarketing calls.

Compliance with these requirements is not burdensome. First the E-Sign Act consent disclosures described above should be displayed on the website in the exact same manner that the TCPA agreement will be displayed, so that when the consumer indicates consent to receive electronic disclosures the consumer is demonstrating the ability to access the TCPA agreement (as required by the E-Sign Act in 15 U.S.C. § 7001(c)(1)(C)). Then, in close proximity to the E-Sign Act disclosures, the consumer should be provided a mechanism to indicate that the consumer agrees to receive information in electronic form—by typing their name, or simply clicking on a box that says, "I agree to receive electronic disclosures." This allows the consumer to provide "affirmative consent" to receive writings electronically, as required by the E-Sign Act.[92]

After the consumer signs the E-Sign consent form, the website can display the TCPA agreement, including the disclosures required by the FCC to be included in the agreements for either consent or permission to receive telemarketing calls. After receiving these disclosures displayed on the website, the consumer can be asked to enter a click or take another electronic action that will

[92] 15 U.S.C. § 7001(c)(1)(A).

meet the requirements for an electronic signature under the E-Sign Act.

3. Oral communications cannot be used to satisfy the FCC's requirement for written agreements for consent and permission.

The E-Sign Act's protections for consumers are especially important when the two parties are *not* transacting online. As was recently demonstrated in a filing by DentalPlans.com, some telemarketers claim that they can provide the written agreement for telemarketing calls verbally over the telephone, and have the consumer provide their signature verbally as well.[93]

As explained *supra,* the E-Sign Act allows a requirement for a written disclosure to be met with an "electronic record" after the E-Sign Act's consent procedures have been followed. However, the E-Sign Act explicitly prohibits an oral record from qualifying as an electronic record for this purpose. Subsection (c)(1) of 15 U.S.C. 7001 explains that writing requirements can be satisfied with electronic records only if the consent procedure in subsection (c) is followed.

> (c)Consumer disclosures
> (1) Consent to electronic records
> Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing **if**—
>
> > (A)the consumer has affirmatively consented to such use and has not withdrawn such consent; . . . .[94]

However, subsection (c)(6) specifically excludes oral communications from qualifying as the electronic records defined in subsection (c)(1) that can replace a disclosure required to be given in writing to a consumer:

> (6) Oral communications
> An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law.[95]

Indeed, allowing consent agreements to be provided in oral communications would corrupt

---

[93] *See* Petition for Expedited Declaratory Ruling Regarding the Application of U.S.C. § 227(b)(1)(B) by DentalPlans.com, CG Docket No. 02-278, at 3-4 (filed Jan. 3, 2023), *available at* https://www.fcc.gov/ecfs/document/101032278712147/1 [hereinafter DentalPlans Petition].

[94] 15 U.S.C. § 7001(c)(1) (emphasis added).

[95] 15 U.S.C. § 7001(c)(6) (emphasis added).

and undermine the essential protections intended by the Commission when it required written agreements in 2012.[96]

4. The E-Sign Act consent process is not optional.

The E-Sign Act consent process is not optional. The FCC does not have the authority to ignore the requirements of the E-Sign Act. In 15 U.S.C. § 7004(d)(1), Congress explicitly limited the ability of federal regulatory agencies to avoid the E-Sign Act consent process. An agency is permitted to do so only if it makes an affirmative finding that jettisoning the consent process "is necessary to eliminate a substantial burden on electronic commerce and will not increase the material risk of harm to consumers."

Such a finding would not be possible for the FCC to make. The E-Sign Act consent process provides a critical protection for consumers in electronic transactions. The Federal Trade Commission and the Department of Commerce reported to Congress that the E-Sign Act requirement is important because it "ensures that consumers who choose to enter the world of electronic transactions will have no less access to information and protection than those who engage in traditional paper transactions."[97] These two agencies noted that the strict use of and compliance with the consumer consent provision is also necessary to protect consumers from the ever-growing use of electronic commerce for fraud.[98] As calls and texts are well-known vehicles for fraud calls and

---

[96] *See* 2012 Report and Order, *supra* note 58, at ¶ 19.

[97] Fed. Trade Comm'n, Electronic Signatures in Global and Nat'l Commerce Act: The Consumer Consent Provision in Section 101(c)(1)(C)(ii) (June 2001), *available at* www.ftc.gov.

The FTC and the Department of Commerce went on to state:

Moreover, this provision reduces the risk that consumers will accept electronic disclosures or other records if they are not actually able to access those documents electronically. As a result, it diminishes the threat that electronic records will be used to circumvent state and federal laws that contain a "writing" requirement. The consumer consent provision in Section 101(c)(1)(C)(ii) provides substantial benefits as a preventive measure against deceptive and fraudulent practices in the electronic marketplace. *Id.*

[98] The electronic marketplace has not been immune to the types of deceptive and fraudulent practices that have plagued the traditional marketplace. In February 2022, the FTC released its annual Consumer Sentinel Network Report detailing consumer complaint data for 2021. The report shows that 49% of all complaints were related to fraud, and of the consumers who identified the company's method of contact, 14% identified email as the specific contact method, 10% identified websites or apps, and 9% identified social media. Federal Trade Comm'n, Consumer Sentinel Network Data Book 2021, at 4, 12 (Feb. 2022), *available a*t www.ftc.gov. Of the consumers who reported fraud complaints against foreign companies and identified the method of contact, 64% said they had also been approached online (which encompasses email, website or apps, and social media). *See* FTC Consumer Sentinel Network, Fraud Reports Against non-U.S. Companies (Contact and Payment Method tab checked), *available*

billions of illegal telemarketing calls,[99] every applicable legal tool should be robustly employed to thwart them.

In 2012, the Commission noted the "ongoing consumer frustration" from unwanted telemarketing calls and found that imposing the writing requirement for consumer consent for prerecorded telemarketing calls "will provide substantial benefits to consumers without substantial implementation costs."[100] Consumer frustration regarding telemarketing calls has only grown in the intervening eleven years, and a primary reason for the growth in these unwanted calls is the callers' use of online "agreements" purporting to provide consent for telemarketing calls. Indeed, some telemarketers attempt to gain verbal consent for telemarketing calls.[101] As a result, to maintain the consumer protections initially intended when the Commission required written agreements in 2012, the Commission should reiterate the current requirement that a written agreement is required for consent and permission even when the transaction to obtain such consent is conducted through electronic means.

D. The FCC should issue guidance explaining how the E-Sign Act's requirements apply to its regulations.

The federal E-Sign Act provides the mechanism that allows an electronic signature to be considered equivalent to a "wet" signature, and an electronic record to satisfy a requirement for a writing. Given the level of confusion relating to the application of the federal E-Sign Act to the requirements for writings and signatures required for consent to telemarketing calls, we ask the Commission to specifically articulate the following:

1. The federal E-Sign Act regulates the replacement of the required signature with an electronic signature. Accordingly, an electronic action can meet the requirement that the consumer sign an agreement to receive prerecorded calls, or telemarketing calls to a DNC line, only if that electronic action meets the definition of an electronic signature in the E-Sign Act at 15

---

at https://public.tableau.com/app/profile/federal.trade.commission/viz/InternationalReports/TopCountries.

[99] *See* Scam Robocalls report, *supra* note 44; Federal Bureau of Investigation, Internet Crime Complaint Ctr., Internet Crime Report 2022, at 16, *available a* https://www.ic3.gov/Home/AnnualReports (showing increase of illegal call centers that defraud thousands of victims each year, responsible for over $1 billion in losses to victims).

[100] 2012 Report and Order, *supra* note 58, at ¶ 19.

[101] *See, e.g.,* DentalPlans Petition, *supra* note 93, at 3-4.

U.S.C. § 7006(5). Thus, when an electronic sound, symbol, or process is used as a signature, it must be attached to or logically associated with the electronic record that includes the agreement, and the electronic sound, symbol, or process must be executed or adopted by a person with the intent to sign the agreement.

2. An electronic signature is valid only if it was made or adopted by the signer, and an electronic signature applied to an agreement regarding calls from one seller cannot be attributed to agreements with sellers listed elsewhere, because that electronic signature would not be attached to an agreement relating to those other sellers, nor would the signer have the requisite intent to agree to receive calls from those other sellers.
3. Since callers have the duty to prove that they have consent for their covered calls, they bear the burden of proving that a consumer's electronic signature attached to an electronic record meets the E-Sign Act's definition of electronic signature.
4. As a separate requirement, whenever a law or regulation requires a consumer to be given information in writing, the E-Sign Act allows it to be delivered electronically only if the consumer has first stepped through a special consent procedure to demonstrate agreement and the ability to receive the information electronically. Unless this E-Sign Act consent process, set forth at 15 U.S.C. § 7001(c), is followed, providing a writing through an electronic record is ineffective. Since the FCC's rules for both prior express written consent and prior express invitation or permission require information to be given to the consumer in writing before the consumer signs, the E-Sign Act's consent process to receive this information electronically must be followed. A consumer's purported consent to receive telemarketing calls through electronic media that does not include the consumer's E-Sign Act consent is invalid.
5. The E-Sign Act provides that an oral communication or a recording of an oral communication cannot be used to satisfy a requirement that information be provided to a consumer in writing, so oral communications are insufficient to meet the requirement of a written agreement giving consent or permission for telemarketing calls. This means that no consent or permission can be granted through a telephone call.

VII. Conclusion.

We very much appreciate the Commission's ongoing efforts to curb illegal and invasive calls and texts. As a large percentage of the agreements providing consent or permission for

telemarketing calls that are the basis for the claims of legality by the telemarketers are fabricated by lead generators, bots, or data brokers, it is incumbent on the Commission to shut down those false justifications for the illegal calls. As we have explained in these extensive comments, the current regulations, when combined with the mandates of the federal E-Sign law, already provide the legal machinery by which this can be done. No new regulations on consent—or permission—for telemarketing calls are necessary. We urge the Commission to follow our recommendations regarding blocking texts, and, in addition to codifying the application of the DNC rules to texts, issue guidance simply reiterating the constraints of the current regulations.

Respectfully submitted, May 8, 2023.

Margot Saunders
Senior Counsel
msaunders@nclc.org
Carolyn L. Carter
Deputy Director
ccarter@nclc.org
National Consumer Law Center
1001 Connecticut Ave., NW
Washington, D.C. 20036

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

Appendix
National Consumer and Privacy Organizations Submitting Comments

National Consumer Law Center (NCLC) is a national research and advocacy organization focusing on justice in consumer financial transactions, especially for low-income and elderly consumers. Attorneys for NCLC have advocated extensively to protect consumers' interests related to robocalls before the United States Congress, the Federal Communications Commission (FCC), and the federal courts. These activities have included testifying in numerous hearings before various congressional committees regarding how to control invasive and persistent robocalls, appearing before the FCC to urge strong interpretations of the Telephone Consumer Protection Act (TCPA), filing amicus briefs before the federal courts of appeals representing the interests of consumers regarding the TCPA, and publishing a comprehensive analysis of the laws governing robocalls in National Consumer Law Center, Federal Deception Law, Chapters 6 and 7 (4th ed. 2022), updated at www.nclc.org/library.

Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., that focuses public attention on emerging privacy and technology issues. EPIC often participates as amicus curiae to explain the technology at issue in a case, and in other federal district courts and appellate courts regarding the Telephone Consumer Protection Act. Additionally, EPIC's attorneys employ their expertise in advocacy before the Federal Communications Commission (FCC), and the Federal Trade Commission to protect consumers' privacy in the electronic sphere. https://epic.org/

Appleseed Foundation is a non-profit, nonpartisan organization dedicated to helping build a world where every person can thrive and where justice is abundant. The Appleseed Foundation facilitates collaboration throughout the **Appleseed Network** of 18 Appleseed justice centers across the US and Mexico. Appleseed partners with communities on research, organizing, advocacy, and litigation to build systemic solutions and advance social justice. https://appleseednetwork.org/

Consumer Action has been a champion of underrepresented consumers since 1971. A national, non-profit 501(c)3 organization, Consumer Action focuses on financial education that empowers low to moderate income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers and regulators to advance consumer rights and promote industry-wide change particularly in the fields of consumer protection, credit, banking, housing, privacy, insurance and telecommunications. www.consumer-action.org

Consumer Federation of America (CFA). Is an association of nearly 300 non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. As a research organization, CFA investigates consumer issues, behavior, and attitudes through surveys, focus groups, investigative reports, economic analysis, and policy analysis. The findings of such research are published in reports that assist consumer advocates and policymakers as well as individual consumers. As an advocacy organization, CFA works to advance pro-consumer policies on a variety of issues before Congress, the White House, federal and state regulatory agencies, state legislatures, and the courts. As an educational organization, CFA disseminates information on consumer issues to the public and news media, as well as to policymakers and other public interest advocates. CFA has participated repeatedly in comments to the FCC on a wide variety of issues concerning the Telephone Consumer Protection Act and has

made recommendations to the FCC regarding robocalls and other TCPA issues as a member of the FCC's Consumer Advisory Council. https://consumerfed.org/

The National Association of Consumer Advocates (NACA) is a nationwide non-profit membership organization of private, public sector, legal services and non-profit attorneys, law professors, and law students whose primary interest is the protection and representation of consumers. NACA is actively engaged in promoting a fair and open marketplace that forcefully protects the rights of consumers, particularly those of modest means. NACA's mission is to promote justice for all consumers by maintaining a forum for communication, networking, and information sharing among advocates across the country, and by serving as a voice for its members and consumers in the ongoing effort to curb unfair, deceptive, and otherwise exploitative business practices. https://www.consumeradvocates.org/

National Association of State Utility Consumer Advocates, (NASUCA) is an association of 60 consumer advocates in 44 states and the District of Columbia Barbados, Puerto Rico, and Jamaica. NASUCA's members are designated by the laws of their respective jurisdictions to represent the interests of utility consumers before state and federal regulators and in the courts. https://www.nasuca.org/ NASUCA's full members are designated by the laws of their respective jurisdictions to represent the interests of utility consumers before state and federal utility regulators and in the courts. NASUCA's associate and affiliate members are recognized utility consumer advocates in their respective jurisdictions. Robocall Resolution 2011-07 - Opposing the Use of Telephone Numbers for Unsolicited Contact Without Affirmative, Prior Consent: https://www.nasuca.org/robo-call-resolution-2011-07/

National Consumers League (NCL). The National Consumers League is America's pioneering consumer advocacy organization, representing consumers and workers on marketplace and workplace issues since our founding in 1899. Headquartered in Washington, DC, today NCL provides government, businesses, and other organizations with the consumer's perspective on concerns including child labor, privacy, food safety, and medication information. https://nclnet.org/

Public Citizen is a non-profit consumer-advocacy organization with a longstanding interest in maintaining the protections that the Telephone Consumer Protection Act (TCPA) provides consumers against unwanted intrusions from telemarketers who use robocalling technology to besiege cell phones and home phones. Public Citizen has submitted comments to the Federal Communications Commission (FCC) on proposals and petitions under consideration by the FCC concerning the TCPA, and it has requested that the FCC issue clarifications and rules addressing consent requirements for receiving prerecorded calls and automated texts under the TCPA and the 2019 Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. https://www.citizen.org/

Public Knowledge is a non-partisan, non-profit consumer rights organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works. It has worked for many years to promote telecommunications policies that protect consumers, and has filed comments to the Federal Communications Commission (FCC) on proposals supporting the protections that the Telephone Consumer Protection Act (TCPA). https://publicknowledge.org/

U.S. PIRG. The PIRG Consumer Watchdog team is working to make sure consumers are informed and empowered to protect themselves in today's rapidly changing marketplace. Our researchers are working to get rid of unsafe products and expose unfair practices, and we're advocating for needed reforms to state and federal consumer protection laws. https://pirg.org/our-work/consumer-protection/