**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, DC 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | CG Docket Nos. 21-402, |
| Targeting and Eliminating Unlawful | ) | 23-107, 02- 278 |
| Text Messages | ) | |
| | ) | |

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

**by**

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

Submitted February 26, 2024

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

## Table of Contents

## Comments

## I. Introduction and Summary

These comments are respectfully submitted by the **National Consumer Law Center,** on behalf of its low-income clients, **Consumer Action, Consumer Federation of America, Electronic Privacy Information Center, National Association of Consumer Advocates, National Consumers League,** and **U.S. PIRG**, in relation to the Federal Communication Commission's (FCC or Commission) Second Further Notice of Rulemaking on addressing unwanted texts.[1] As we describe in **Section II**, the amount of money lost by consumers to scam texts continues to climb, compelling the FCC to adopt more aggressive regulations that will eliminate many more scam texts.

On behalf of a broad coalition representing consumers, we have submitted comments in all of the Commission's proceedings relating to stopping dangerous and unwanted texts.[2] In each proceeding, we have urged the Commission to consider ways to provide **financial incentives to text service providers** (including both the initiating and the terminating providers) so that they will implement practices that safeguard consumers from the risks of scam texts. We have pointed out that losses to consumers resulting

---

[1] *In re* Targeting and Eliminating Unlawful Text Messages; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991; Advanced Methods to Target and Eliminate Unlawful Robocalls, Second Report and Order, Second Further Notice of Proposed Rulemaking in CG Docket Nos. 02-278 and 21-402, and Waiver Order in CG Docket No. 17-59, CG Docket Nos. 21-402, 02-278, & 17-59 (Rel. Dec. 18, 2023), *available at* https://docs.fcc.gov/public/attachments/FCC-23-107A1.pdf [hereinafter Second FNPRM]; Targeting and Eliminating Unlawful Text Messages; Implementation of the Telephone Consumer Protection Act of 1991, Proposed Rule, CG Docket Nos. 02-278, 21-402, 89 Fed. Reg. 5177 (Jan. 26, 2024), *available at* https://www.govinfo.gov/content/pkg/FR-2024-01-26/pdf/2023-28833.pdf.

[2] In our first comments in this proceeding (submitted November 10, 2022), we urged the Commission to prioritize the protection of consumers from scam texts and consider how to shield consumers from non-SMS text messages. *In re* Targeting and Eliminating Unlawful Text Messages, Comments of Electronic Privacy Information Center, National Consumer Law Center et al. on Notice of Proposed Rulemaking in CG Docket No. 21-402, CG Docket No. 21-402 (filed Nov. 10, 2022), *available at* https://www.fcc.gov/ecfs/document/11110142720936/1.

In our Reply comments (filed on behalf of 16 national and state consumer advocacy organizations, submitted December 9, 2022), we urged the Commission "to create and enforce incentives that will assist in limiting scammers' use of texts as a tool to defraud vulnerable consumers. . . ." *In re* Targeting and Eliminating Unlawful Text Messages, Reply Comments of National Consumer Law Center et al. on Notice of Proposed Rulemaking in CG Docket No. 21-402, CG Docket No. 21-402 (filed Dec. 9, 2022), *available at* https://www.fcc.gov/ecfs/document/12092983121644/1.

On May 8, 2023, we filed comments on behalf of 11 national consumer and privacy organizations in which we emphasized that the Commission must "act forcefully to stop the unrelenting onslaught of . . . unwanted texts to American telephones." *In re* Targeting and Eliminating Unlawful Text Messages; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Comments of National Consumer Law Center et al. Relating to the Report and Order and Further Notice of Proposed Rulemaking Issued March 17, 2023, CG Docket Nos. 20-402 & 02-278, at 2-3 (filed May 8, 2023), *available at* https://www.fcc.gov/ecfs/document/1050859496645/1.

from scam texts increased by 400% over a four-year period.[3] And, we have repeatedly requested that the Commission **prioritize protecting consumers from scams over protecting the income to text providers.**

In its most recent Order (released on December 18, 2023),[4] the Commission implemented some new requirements to protect consumers from scam texts. We appreciate the Commission's continued efforts to address these issues and encourage the Commission to adopt even stronger mechanisms to effectively stop scam texts.

In the current FNPRM, the Commission proposes somewhat more aggressive measures than those adopted thus far. But, as we explain in **Section III**, without essential changes to the timing of Commission notices and orders, among other things, we believe it is unlikely that these proposals will be sufficient to stop scam texts from annoying cell phone users and providing the vector for fraudsters to steal hundreds of millions of dollars from consumers. We illustrate in this Section how even while the majority text platforms are able to avoid transmitting the scam texts, many large platforms that transmit the scam texts also transmit tens of thousands legitimate texts from business texters. We urge the Commission to create meaningful incentives for text platforms to eliminate their transmittal of all illegal texts.

In **Section IV**, we describe how the Commission should encourage banks and other major business texters whose texts are used by fraudsters to leverage their marketplace power and insist that the platforms that transmit their texts do not also transmit scam texts. Additionally, we urge the Commission to identify a technology that allows consumers to trust the origin of the texts they receive.

The overriding goal of these comments is to urge the Commission to:

- **Prioritize the protection of consumers from scam texts.**
- **Provide effective incentives to text providers to stop the scam texts.**
- **Encourage legal texters to ensure that the platforms that transmit their texts do not transmit scam texts.**
- **Explore technological and other means to allow consumers to know when to trust their text messages.**

[3] NCLC's May 8, 2023 comments, *supra* note 2, at 2.

[4] Second FNPRM, *supra* note 1.

## II. Scam texts are still a major problem that the Commission must address aggressively.

Although some commenters may claim that the texting industry has largely resolved the problem of scam texts, the fact is that, in 2023 there were 230,407 reports of text scams to the Federal Trade Commission ("FTC"), resulting in $372 million in losses.[5] While the total number of reports is down from the year before, the amount of money reported lost increased by 12.7% from 2022.[6]

In its most recent report, Robokiller notes that "Robotexts are far and away the leading scam threat."[7] Robokiller reports that, in every month in 2023, more than 10 billion spam texts were sent, reaching a high of more than 19 billion in January of 2024.[8] Its 2023 mid-year report indicates an 18% increase between 2022 and 2023.[9] It estimates over $20 billion in losses due to robotext scams in 2022.[10]

Truecaller has also consistently reported high numbers for spam texts from 2019 through 2022, at least 25 per person per month[11] (it did not produce an annual report in 2023). On the business side, cybersecurity company Proofpoint has indicated that 75% of organizations surveyed in 2021 and again in 2022 reported encountering at least one SMS-based scam,[12] with 41% of working adults surveyed in the United States reporting they received at least one suspicious text message on their phone.[13]

These numbers indicate that much more needs to be done to stop scam texts.

---

[5] FTC Consumer Sentinel Network, Fraud Reports by Contact Method (data as of Dec. 31, 2023), *available at* https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts.

[6] *Id.*

[7] Robokiller, The Robokiller Phone Scam Report: 2022 Insights and Analysis 2, *available at* https://assets.website-files.com/61f9a8793a878d7f71c5505d/6400e06e514500224ad26830_The%20Robokiller%20phone%20scam%20report%20-%202022%20insights%20%26%20analysis.pdf.

[8] Robokiller, 2023 United States Robotext Trends, *available at* https://www.robokiller.com/spam-text-insights#introduction (19.2 billion spam texts in January 2024).

[9] Robokiller, The Robokiller Phone Scam Report: 2023 Mid-Year Insights & Analysis 4, *available at* https://assets.website-files.com/61f9a8793a878d7f71c5505d/64ca6ccf1f5e962fae3e55e3_Robokiller%20Mid-Year%20Report%202023.pdf.

[10] *Id.*

[11] Truecaller, Truecaller Insights 2022 U.S. Spam & Scam Report, *available at* https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report ("Monthly Spam Received").

[12] Proofpoint, 2023 State of the Phish 12, *available at* https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2023.pdf.

[13] Proofpoint, 2022 State of the Phish 57, *available at* https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2022.pdf.

## III. Blocking texts from providers will be helpful, but the process must be sped up to be most effective.

### A. The Commission should establish a process that requires the blocking of texts from texting providers within 48 hours after they are notified that they are transmitting scam texts, unless the scam texts have been eliminated.

Among other things, the Commission asks about whether originating text providers should be required to block all texts from a particular source after Commission notification of scam texts.[14] Alternatively, the Commission asks whether to "require originating and/or terminating providers to block using the 'substantially similar' standard applied in our call blocking rules[.]"[15]

We strongly support requiring both originating and terminating providers to block texts form a particular source after Commission notification of scam texts. But more importantly, we urge the Commission **to establish a process requiring the blocking, in a swift and efficient manner, of all texts from a particular provider that is transmitting scam texts.** The threat of a disruption of service for providers who continue to transmit scam texts would provide important incentives for all providers to ensure that their platforms are scam-free. **We suggest that the Commission should order that all texts be blocked from a provider within 48 hours after notification, unless the provider can demonstrate that the scam texts were eliminated.**

NCLC recently engaged YouMail[16] to evaluate the originating platforms for text messages it determined to be scam messages. YouMail harvests information on robocalls and texts sent to both its more than 13 million registered users, and approximately 10 million additional active other numbers. Using this information, it can identify the text providers that are transmitting illegal texts.

On February 26, 2024, YouMail gave NCLC the following statement, with permission to include this statement in these comments:

> Pursuant to a contractual arrangement between YouMail and the National Consumer Law Center, YouMail examined SMS messages received by its Android and iPhone customers between November 1, 2023, and February 15, 2024, carrying content identified by its customers and threat analysts categorized as both spam text messages and scam text messages.
>
> The process used in this analysis led us to evaluate the content of over 100 originating messaging platforms to determine which platforms were responsible for originating the

[14] Second FNPRM, *supra* note 1, at ¶ 68.

[15] *Id.* at ¶ 72.

[16] YouMail provides investigative and analysis services to the FCC, FTC, Department of Justice, and state attorneys general, as well as numerous private industries and individual companies, including banks, retail services, and CTIA and US Telecom.

identified spam and scam text messages. These platforms included some of the largest text providers in the communications industry, as well as many smaller providers.

As of February 25, 2024, YouMail had preliminary results of this investigation. YouMail observed the following:

**Spam Content.**

1. For 15% of the providers, 1 out of 5 text messages or more (20% or more) originating from the platform was spam.
2. For 29% of the providers, 1 out of 10 text messages or more (10% or more) originating from the platform was spam (inclusive of the 15% identified in #1).
3. These identified providers also transmitted large numbers of legitimate texts from enterprises, including banks, retailers, and others.
4. For 5% of the providers, over half of their traffic appeared to be spam.
5. For 23% of the providers, there were no observable text messages carrying content that consumers would generally regard as spam.

**Scam Content**.

6. For 21% of the providers, 1 out of 100 text messages originating from the platform carried content believed to be a scam.
7. As these identified providers also transmitted large numbers of legitimate texts from enterprises, including banks, retailers, and others, although the percentage of scam messages was relatively small, the total number of scam texts transmitted appears to be significant.
8. For a subset of the providers identified in # 6, a substantial proportion of their traffic are believed to be scams.
9. For 62% of all 100 providers included in the review, there were no observable text messages carrying content believed to be a scam.[17]

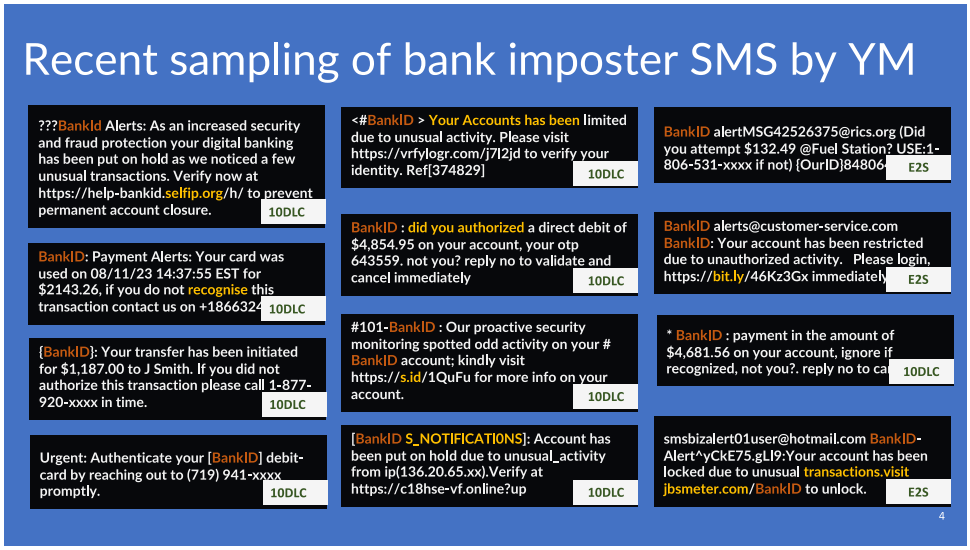
YouMail's analysis illustrates three important points. First, the providers that are primarily transmitting illegal texts can be clearly identified. Second, some of the providers of text services to businesses that are sending entirely legal—and desired—texts are also transmitting scam texts. Third, as the majority of providers—62% (point #9 from the YouMail statement)—are able to avoid sending scam texts, providers clearly have this capability. This means that those who do continue to transmit scam texts should be punished for continuing to do so.

We understand that the Commission has access to YouMail's data reporting about which providers are transmitting scam texts. **We urge the Commission to use this data regularly and develop a process to require the blocking of all texts sent by providers that continue to transmit scam texts 48 hours after notice from the Commission.**

[17] This statement was provided to NCLC on February 25, 2024 and updated on February 26, 2024.

No need exists for a prolonged process between the time the Commission first provides notice to a provider to stop transmitting scam texts and the time an order requiring blocking of all texts from that platform is issued. As the Commission notes, the content of texts is easily accessible by all involved in the transmittal process.[18]

Scam texts are fairly easy to identify. Here is an illustration—also provided by YouMail—of multiple recent bank imposter texts, all of which YouMail has determined to be scams. The platforms and providers transmitting these imposter texts can see them—and prevent them—if they choose to do so.




The Commission notes that triggering the procedure for blocking all traffic from a voice service provider after Commission notification is a "detailed process,"[19] and asks whether this detailed process is appropriate for scam texts. In our opinion, the answer is no.

We urge the Commission to speed up the text blocking process. It is important to note that during the pendency of the Commission's blocking process, tens of thousands of scam texts will assault consumers, some of whom will fall for the ruses, and will lose money to the fraudsters. The Commission should order all text traffic from a provider to be blocked if the provider continues to transmit scam text messages 48 hours after notice from the Commission that it is transmitting scam texts.

It is wrong to allow a text provider to continue transmitting scam texts after it has been notified by the Commission to stop. The days and weeks involved in the Commission's standard process are unnecessary here. And allowing the scam texts to continue for days and weeks *after* the Commission has

[18] *Id.*

[19] *Id.* at ¶ 73.

notified the provider to stop is extremely harmful to consumers. The Commission must prioritize the safety of America's cell phone users over the income of the text platforms found to be continuing to transmit scam texts.

The alternative mechanisms available to consumers during the interim period between the Commission's notification and the blocking order are the "Report Junk" option included on some texts,[20] and the option to dial "SPAM" [21] and report the text to one's cell phone provider. While these mechanisms are likely helpful to the overall effort of dealing with unwanted texts, they are clearly not sufficient to stop the scam texts. First, scam texters will not include the "Report Junk" message in their texts. Second, these mechanisms provide no way to distinguish between dangerous scam texts and just annoying and unwanted ones. Moreover, reports from these two mechanisms are provided only to the reporting consumer's provider, and—alarmingly—providers are under no legal obligation to react to these reports, and they have been known to take weeks to block numbers sending dangerous scam texts.

### B. Providers should be required to pay heavy fines if they transmit scam texts for more than a few days, without prior notice from the Commission.

Every text transmitted by a provider represents a source of income to the multiple parties involved in the transmission and delivery of texts.[22] To incentivize providers to stop transmitting scam text messages, the Commission must make it more expensive for them to transmit illegal texts compared to the revenue they receive from those texts. This means that providers must face significant—and likely—financial costs if they allow texts to be transmitted over their networks. In short, the risks must be more significant than the benefits.

The Commission's proposal "to require all immediate downstream providers to block the texts from providers that fail to block after Commission notification"[23] would create valuable incentives to providers to pay attention and cut off spam texters *after notification from the Commission.* But there are over 6 billion texts sent every day through this nation's telephone system.[24] Providing this costly punishment only

---

[20] CTIA, Messaging Principles and Best Practices 7.2.1.2 (May 2023), *available at* https://api.ctia.org/wp-content/uploads/2023/05/230523-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf.

[21] Federal Trade Comm'n, Consumer Advice, How to Recognize and Report Spam Text Messages, *available at* https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages.

[22] Providers are paid $.015 to $.016 for each text, depending upon the type and the length. *See, e.g.*, Omnisend, Send Email & SMS That Really Sell, *available at* https://www.omnisend.com/blog/sms-marketing-pricing/ ; https://simpletexting.com/blog/cost-of-mass-texting/.

[23] Second FNPRM, *supra* note 1, at ¶ 68.

[24] Adnan Olia, Intradyn, Text Message Statistics & Trends for 2024 [And Beyond!], *available at* https://www.intradyn.com/text-message-statistics-trends/#:~:text=sent%20per%20day%3F-

*after* the guilty provider is caught the second time transmitting these illegal texts fails to create incentives to providers to be careful *before they are caught and notified by the Commission.*

Here is an analogy: How effective would laws against speeding and driving while intoxicated be if punishments were applied only after the driver was caught the second time? Every driver would know that they could drive with impunity (with only their conscience and fear to provide limits) until they were caught the first time. The answer is that there would be a lot more traffic deaths because drivers who had not been caught the first time would feel able to drive as fast and as recklessly as they dared.

But the U.S. system of regulating drivers imposes sanctions immediately after the first time a driver is caught, in the form of a ticket, fines, and likely increased mandatory insurance rates.[25] The consequences are more costly the second time a driver is caught, even leading to suspension of one's driver's license, or such a steep increase in the price of insurance that makes it unaffordable.[26] The first ticket is often sufficient to encourage drivers to slow down and stop driving while impaired, so that they do not get that second ticket.[27]

Currently, because of scam detection service providers such as YouMail and other venders, the Commission can see which text providers are responsible for transmitting scam texts. These text providers should not be permitted to continue to profit from transmitting the scam texts *until* the Commission sends them a notice.

We recommend that the Commission develop a protocol for punishing text platforms for transmitting scam texts for more than a few days—even before they are notified by the Commission. Given the fact that the majority of text platforms successfully identify and exclude scam texts from their platforms, the platforms that do not exercise these precautions should be punished. In this society, we punish speeders the first time they are caught. Platforms that participate and profit from scam texts should also be punished the first time they are caught. If the provider can show that the scam texts were allowed into their system in error, and that the provider eliminated the illegal texts within a few days, that might be sufficient to avoid the fine or the temporary blocking. But the burden should be on the text provider to

---

,Mobile%20phone%20users%20in%20the%20U.S.%20alone%20sent%202%20trillion,are%20sent%20worldwide%20each%20day.

[25] *See* Susan Meyer, The Zebra, *The Most Common Traffic Tickets in the U.S.* (updated Sept. 1, 2023), *available at* https://www.thezebra.com/resources/driving/common-traffic-tickets/.

[26] *See* Sexner & Associates, L.L.C., What Happens If You Get Multiple Speeding Tickets?, *available at* https://sexner.com/blog/what-happens-if-you-get-multiple-speeding-tickets/.

[27] *See* Nosal & Jeter, L.L.P., The Effects of Traffic Tickets on Motorist Behavior, *available at* https://trafficlawsc.com/the-effects-of-traffic-tickets-on-motorist-behavior/.

show that it was on guard, employing robust anti-scam tools, which failed only temporarily, to excuse punishment for transmission of the scam texts.

### C. We support the Commission's proposal to require that email-to-texts be opt in.

All of the bank imposter texts illustrated above were sent either using 10-digit local numbers or email-to-text mechanisms. We applaud the Commission's proposal to require providers to make email to text opt-in for customers. However, we urge the Commission to require providers to explain to their customers the dangers of accepting email to texts when they notify them of this choice.

We also urge the Commission to encourage banks and other major business texters whose texts are used by fraudsters to scare and cheat consumers to leverage their marketplace power and insist that the platforms that transmit their texts do so only through providers that do not also transmit these scam texts. We describe this mechanism more in the following Section IV.

## IV. The Commission should encourage legal callers to leverage their marketplace power to protect their texts from blocking and ensure they are delivered.

As we have explained, requiring blocking of the texts from text providers only after they have been identified by the FCC seems unlikely to change the basic dynamic that drives these illegal texts: the providers are making sufficient income from these messages to make it more profitable to keep making the texts and risking the punishment. Clearly, the potential for costly consequences from conveying illegal messages is sufficiently remote and outweighed by the income from these texts such that the current measures fail to dissuade these providers from continuing their current practices.[28]

We have previously submitted comments[29] in the robocall proceedings in which we have urged the Commission to adopt a set of best practices for legal callers that we believe—if widely used—will likely eliminate many of the illegal calls plaguing subscribers' telephone lines. These best practices would leverage the market power of the legal callers to change the calculus of service providers that are currently

[28] This dynamic was noted in 2021 by Commissioner Starks: "[I]llegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it." *In re* Call Authentication Trust Anchor, Further Notice of Proposed Rulemaking, WC Docket No. 17-97 (Sept. 30, 2021) (Statement of Comm'r Geoffrey Starks).

[29] *See In re* Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor, Reply Comments of National Consumer Law Center, Electronic Privacy Information Center, & Public Knowledge Relating to the Seventh Report and Order and Eighth Further Notice of Proposed Rulemaking Issued May 19, 2023, CG Docket No. 17-59, WC Docket No. 17-97 (filed Sept. 8, 2023), *available at* https://www.fcc.gov/ecfs/document/10908314166629/1.

complicit—either knowingly or with deliberate blindness—about their transmission of illegal messages. We also encourage the adoption of these best practices for text messages.

Consumers want and often rely on the calls and texts from some businesses: banks, health care providers, and others, to alert them to real threats to their health or financial affairs. Consumers fall prey to the messages sent by scammers pretending to be these businesses because there is no simple way for consumers to tell which are the scams. No safe means currently exist to know who is on the other end of the call or who really sent that text.

We urge the Commission to engage in an evaluation of technology to establish a reliable method for these businesses to send their text messages that would assure consumers that texts coming through that pathway can be relied upon to be what they seem. This is especially important given the large number of scam texts that are sent through alternative technologies, such as IMessage, Google Message, and Over the Top applications, such as WhatsApp and Facebook Messaging, which are invisible to the consumers' providers. Few consumers understand the different risks inherent in the various mechanisms. Consumers need an easy way to identify which messages are safe for them to open. The Commission should lead the way in creating a safe pathway and educating consumers about it.

Until such a reliable method has been identified, legal texters could ensure that their messages are reaching intended recipients by imposing strict requirements on the platforms and providers that they engage to originate and transmit their messages. Through contractual requirements, they could demand that the providers that transmit their messages must not also transmit any scam messages. They could ascertain compliance by their providers by evaluating the data made available by YouMail and similar companies. And they could threaten financial consequences to those providers if they violate contractual provisions by mixing the texts from these businesses with scam texts.

If the businesses that send legitimate text were to employ these practices, it would force many text providers to avoid transmitting illegal messages, and the profit from illegal messages would plummet. Even more importantly, the illegal texts would no longer be mixed with the legal ones, making it much easier for the terminating providers to identify and block scam texts.

A market-based approach like this would a) provide strong financial incentives to originating and intermediate providers to avoid transmitting illegal messages; b) facilitate the transmission of legal messages through paths that would eliminate the likelihood that the messages would be labeled improperly or blocked by downstream or terminating providers; and c) supplement the other mechanisms created by the Commission intended to address illegal messages.

## V. Conclusion

We very much appreciate your consideration of our views on behalf of consumers. We would be happy to provide further information.

Respectfully submitted:

Margot Saunders
National Consumer Law Center
1001 Connecticut Ave. NW
Washington, D.C. 20036
msaunders@nclc.org