National Consumer Law Center
Fighting Together for Economic Justice

NATIONAL HEADQUARTERS
7 Winthrop Square, Boston, MA 02110
(617) 542-8010

WASHINGTON OFFICE
Spanogle Institute for Consumer Advocacy
1001 Connecticut Avenue, NW, Suite 510
Washington, DC 20036
(202) 452-6252

NCLC.ORG

March 29, 2024

Mr. Barry Wides
Ms. Heather Brown
Office of the Comptroller of the Currency
400 Seventh St. SW
Washington, D.C. 20219

Sent by Email

Re: Follow up information on how banks can stop bank imposter texts

Dear Barry and Heather:

Thank you again for attending our Zoom meeting in February on steps that the banks can take to help stop bank imposter texts. This letter is to provide additional information about the issues that we discussed.

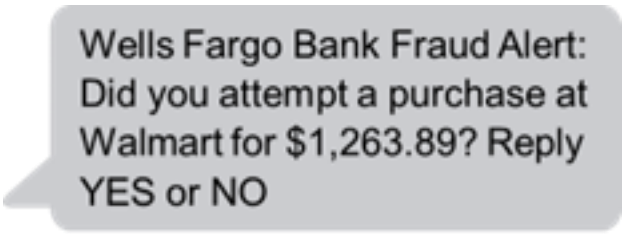
- Section 1 describes the problem with bank imposter texts.
- In section 2, we explain how technology and service providers can identify which text platforms are responsible for originating and sending scam texts.
- Section 3 outlines some safe texting protocols that banks could follow that we believe would substantially help eliminate many of the bank imposter texts.
- Finally, Section 4 relates the steps that we are urging the FCC to take to facilitate the elimination of scam texts.

1. Bank imposter texts are a major problem for banks and consumers.

As you know, bank impersonation texts are one of the most-reported text message scams.[1] Far too frequently, consumers are receiving text messages like this:

If you reply to a text like this, you'll get a call from the (fake) fraud department. People say they thought the bank was helping them get their money back. Instead, money was transferred *out* of

[1] https://www.ftc.gov/news-events/news/press-releases/2023/06/new-ftc-data-analysis-shows-bank-impersonation-most-reported-text-message-scam



their account. This scam's median reported loss was $3,000.

The FTC announced last year that these scams accounted for $330 million in reported losses in 2022.[2] The FTC website explains how these scams typically work:

> [F]ake bank security messages, often supposedly from large banks like Bank of America and Wells Fargo, were the most common type. These texts are designed to create a sense of urgency, often by asking people to verify a large transaction they did not make. Those who respond are connected to a fake bank representative. Reports of texts impersonating banks have increased nearly twentyfold since 2019.[3]

The FTC data reflects only the *reported* losses. The actual losses from texts impersonating banks are generally considered to be much higher. In its most recent report, Robokiller notes that "Robotexts are far and away the leading scam threat."[4] 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.[5] Its 2023 mid-year report indicates an 18% increase between 2022 and 2023.[6] It estimates over $20 billion in losses due to robotext scams in 2022.[7]

Truecaller has also consistently reported high numbers of spam texts from 2019 through 2022, at least 25 per person per month[8] (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,[9] with 41% of working adults

---

[2] *Id.*

[3] *Id.*

[4] 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.

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

[6] 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.

[7] *Id.*

[8] 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").

[9] 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.

surveyed in the United States reporting they received at least one suspicious text message on their phone.[10]

2. The text platforms that transmit scam texts can be identified and *avoided.*

When we met with you last month, we were armed with information about how YouMail,[11] and probably other services, can identify the *voice* service providers that are transmitting scam *calls* to U.S. telephone numbers. After our meeting with you, NCLC engaged YouMail to evaluate the originating platforms for *text messages* it determined to be scam messages.[12]

On February 26, 2024, YouMail gave NCLC the following statement, with permission to include this statement in our comments to the Federal Communications Commission (FCC) and to others:

> 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 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.

[10] 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.

[11] 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.

[12] 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.

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.[13]

YouMail's analysis illustrates three important points. First, some providers are primarily transmitting illegal texts, and they can be clearly identified (point # 8). Second, some of the providers of text services to businesses that are sending entirely legal—and desired—texts are also transmitting scam texts (point # 7). Third, as the majority of providers—62% (point #9)—are able to avoid sending scam texts, providers clearly have this capability. This means that it is feasible and appropriate for banks to avoid using those providers who continue to transmit scam texts.

3. The OCC should require—or at least encourage—all banks to employ safe texting protocols.

Unfortunately, to the text providers that are transmitting both the legal and the illegal texts, currently the costly consequences to text platforms for conveying illegal messages is sufficiently remote that it is outweighed by the income from these texts. As a result, the current measures fail to dissuade these providers from continuing their current practices.[14]

However, we ask that the OCC consider whether it can require, or at least strongly encourage, banks to employ safe texting protocols that leverage their power in the marketplace to isolate the platforms that continue mixing legitimate messages from banks with scam messages.

Consumers want and rely on the calls and texts from their banks to alert them about necessary actions to avoid fees or to real threats to their financial affairs. Consumers fall prey to the messages sent by scammers pretending to be their banks because there is currently no simple way for consumers to tell which are the scam texts.

---

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

[14] 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).

A. It is hard for consumers to discern the real texts from the scam texts.

Texts can be sent in multiple ways. Some are much less expensive than others, and therefore more prone to be used by illegal texters.

1) **10-digit numbers**: Platforms charge the least for these texts, and we are told by YouMail that these often are used for scam texts.

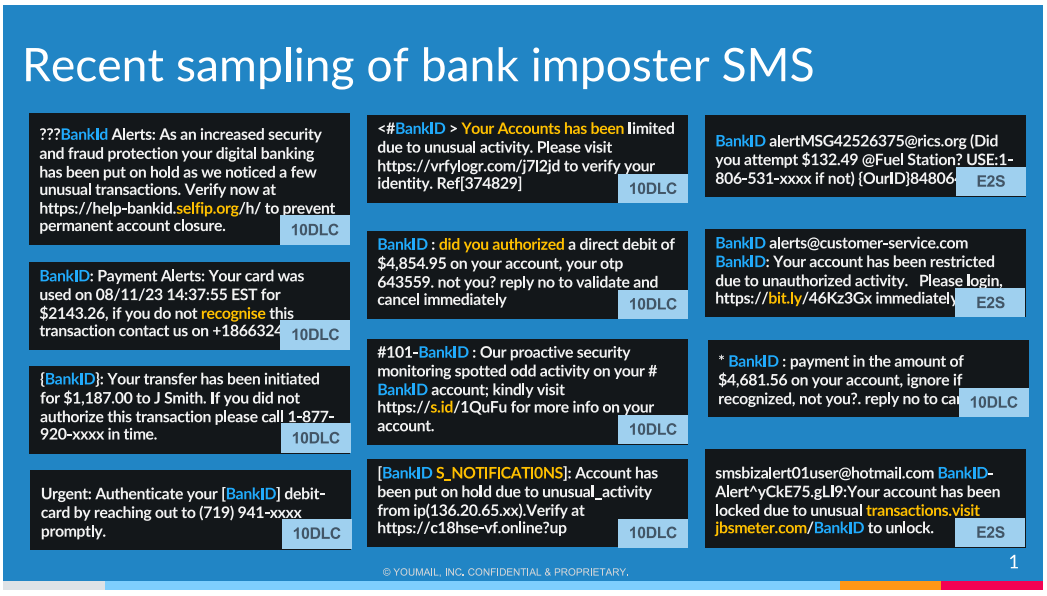
2) **Toll free numbers**: Texts sent using toll free numbers are also fairly inexpensive, and they are also often used for scam texts.

3) **Short codes**: Short codes are 5 or 6-digit numbers that are registered by a single database administered by the CTIA (the trade association for wireless providers).[15] The CTIA and its members maintain compliance guidelines for users of short codes.[16]

4) **Over-the-Top Apps**: These are applications like WhatsApp, Instagram messenger, Google Hangouts, We Chat. There is no meaningful way for texts over these channels to be monitored, and we understand that these channels are often used for scams.

5) **Email to text.** Email to text is the least expensive mechanism to blast texts to multiple recipients, and is often used by scammers.

Below is a slide provided to us by YouMail that illustrates 12 different scam text campaigns.



[15] Short Code Registry, *available at* https://www.ctia.org/programs#:~:text=Short%20Codes%20are%20five%2D%20or,as%20coupons%20or%20news%20updates.

[16] CTIA, Short Code Monitoring Program Handbook, August 2, 2023, *available at* https://api.ctia.org/wp-content/uploads/2024/01/CTIA-Short-Code-Monitoring-Handbook-v1.9-FINAL.pdf.

All of the bank imposter texts illustrated above were sent either using 10-digit local numbers or email-to-text mechanisms. The FCC is poised to require that wireless providers require that their customers opt in to receive these types as texts as an effective way to eliminate this channel.[17] But scammers can continue to use 10-digit numbers and toll free numbers to send texts. And, recipients do not discern the differences when these numbers are sent as standard texts versus those sent as an I-Message or a Google message, or even when the texts are sent through an Over-the-Top App. But none of the scam bank imposter texts were sent using short codes. Further, although we asked YouMail to search for scam texts sent using short codes, they were unable to find any in the past several months. So, it appears that the CTIA compliance guidelines are effective in eliminating the use of short codes for scam texts. This non-governmental system has been largely successful lately in ensuring that short codes are not used to originate scam texts.[18] Additionally, text messages sent by short codes have the advantage of being instantly recognizable to recipients and distinguishable from all other types of texts.

B. Safe texting protocols for banks would involve three steps:

1) **Using market power to isolate scam texts.** Banks should require that the platforms that originate and transmit their texts guarantee not to transmit illegal texts. As over 62% of the text platforms (see section 2, *supra)* are able to avoid transmitting scam texts, avoiding those platforms is clearly possible. If the banks required the platforms they use to avoid sending illegal texts, that would further isolate the platforms that do transmit the illegal texts, making it easier for the illegal texts to be blocked, and the FCC to punish those platforms.

2) **Use short codes only for texts that require higher security.** For those texts that alert the recipient of a pending action which *requires a response* (such as a question about authorizing transfers) the banks should only use the highly monitored short codes.

3) **Promote texts from short codes as the safe texts.** Banks should inform their customers—prominently and repeatedly—that they should only respond to texts from them when the text is sent from a short code. As short codes are easily discernable from both 10 digit codes and toll free numbers, this enables customers to be able to easily recognize which texts are more likely to be scams.

Banks send a lot of texts. Many texts are simply to verify identity. Other texts are simply reminders or notices (such as a bill is due or a threshold in withdrawals or account balance has been reached). But some texts call for a response by the customer directly to the bank, regarding whether a

---

[17] *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, at ¶ 29.

[18] This information came from YouMail.

withdrawal is authorized by the customer.[19] **Those are the texts that banks must ensure are only sent using short codes.**

Finally, the banks should notify their customers repeatedly—on their websites, in all statements and bills, and on prominent signs in their branches—that text notices from banks that require a reply will only be sent using short codes. However, it would be optimal for banks to use short codes exclusively, so that recipients can trust that short code messages are truly from their bank.

4. The FCC can do more to stop scam texts.

NCLC[20] recently filed extensive comments with the Federal Communications Commission (FCC) [21] urging it to take the following steps to address scam texts:

- Prioritize the protection of consumers from scam texts over delivery of potentially illegal messages.
- 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.

We also pointed out that the platforms transmitting the illegal texts need strong financial incentives to change their behavior and forego the income from the scam texts.

We are hopeful that the FCC will decide to act much more quickly and more aggressively to stop scam texters. We are describing our advocacy on this issue briefly here in case the OCC agrees with these arguments, in which case it would be helpful for the OCC to make those points directly to the FCC.

The Commission's recent proposal "to require all immediate downstream providers to block the texts from providers that fail to block after Commission notification"[22] 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 the country's telephone system.[23] Imposing

---

[19] https://www.cnet.com/personal-finance/fake-or-for-real-how-to-know-if-a-text-from-your-bank-is-legit/

[20] On behalf of our low-income clients, as well as Consumer Action, Consumer Federation of America, Electronic Privacy Information Center, National Association of Consumer Advocates, National Consumers League, and U.S. PIRG.

[21] *In re* Targeting and Eliminating Unlawful Text Messages, Comments of National Consumer Law Center, Consumer Action, Consumer Federation of America, Electronic Privacy Information Center, National Association of Consumer Advocates, National Consumers League, and U.S. PIRG, on Notice of Proposed Rulemaking in CG Docket No. 21-402, CG Docket No. 23-107, CG Docket No. 02-278 (filed Feb. 26, 2024), *available at* https://www.fcc.gov/ecfs/document/102260762423180/1.

[22] Second FNPRM at ¶ 68.

[23] Adnan Olia, Intradyn, Text Message Statistics & Trends for 2024 [And Beyond!], *available at* https://www.intradyn.com/text-message-statistics-

this costly punishment only *after* the guilty provider is caught the second time 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.[24] 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.[25] 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.[26]

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

---

trends/#:~:text=sent%20per%20day%3F-,Mobile%20phone%20users%20in%20the%20U.S.%20alone%20sent%202%20trillion,are%20sent%20worldwide%20each%20day.

[24] *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/.

[25] *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/.

[26] *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/.

Conclusion.

We very much appreciate your time and consideration of these ideas. We would be happy to discuss this further with you if that would be helpful.

Sincerely,

Margot Saunders
Senior Counsel
msaunders@nclc.org

Lauren Saunders
Associate Directors
lsaunder@nclc.org