

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

In the Matter of)	
)	
Advanced Methods to Target and Eliminate Unlawful Robocalls)	CG Docket No. 17-59
)	
Call Authentication Trust Anchor)	WC Docket No. 17-97
)	

**REPLY COMMENTS ON
FIFTH FURTHER NOTICE OF PROPOSED RULEMAKING IN
WC DOCKET NO. 17-97**

by

**Electronic Privacy Information Center
and
National Consumer Law Center on behalf of its low-income clients**

Submitted September 16, 2022

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

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

Comments

I. Introduction – The Community Must Stop Scam Robocalls As Soon As Possible

The **Electronic Privacy Information Center (EPIC)**, and the **National Consumer Law Center (NCLC)** on behalf of its low-income clients, file these reply comments to encourage the Commission to prioritize protecting consumers from widescale, automated fraud facilitated through robocalls placed through the U.S. telephone network. We urge the Commission to create meaningful incentives to all providers to stop transmitting illegal robocalls.

In our comments filed last month, we urged the Commission to issue regulations that are more aggressive, more automated, and which effectively motivate providers to avoid transmitting these calls.¹ In these Reply Comments, we are highlighting two problems with the Commission's response to the robocall scourge: inadequate incentives for providers to stop transmitting the calls, and inadequate responsiveness to the harm suffered by consumers.

We do not believe that the exact mechanisms that will quickly stop illegal robocalls from reaching their targets need to be spelled out by Commission. It is clear, however, that there are mechanisms that providers can use that can meaningfully stop most, if not all, of the illegal calls from reaching subscribers.² Providers will be financially motivated to comply with the law if punishments are swift, certain, and sufficiently severe against those providers found to have been complicit. Given the proper incentives, the communications industry in the United States will

¹ See Comments of EPIC and NCLC, *In re Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 (Aug. 17, 2022), <https://www.fcc.gov/ecfs/search/search-filings/filing/10817350228611>.

² For example: YouMail's efforts to assist the Social Security Administration (SSA), *see id.* at 12, and the Commission requiring downstream providers to block traffic from bad actors transmitting large volumes of illegal auto warranty calls, *see* Press Release, Yost Files Suit Alleging Massive Robocall Scheme – FCC Joins Fight in Related Action (Jul. 7, 2022), <https://www.ohioattorneygeneral.gov/Media/News-Releases/July-2022/Yost-Files-Suit-Alleging-Massive-Robocall-Scheme-F>.

develop and implement additional successful mechanisms as they become necessary. We and others have proposed several mechanisms in other filings.³

II. Incentivize Providers to Effectively Eliminate Scam Robocalls

The Commission is uniquely positioned to require proactive, immediate, effective mitigation. We are concerned that the Commission’s current methodology of addressing the problem relies too much on individual enforcement actions rather than on automated, systemized responses. The sheer number of illegal campaigns mounted monthly—by some estimates nearly 2,000 scam robocall campaigns—means that relying on individual enforcement actions is unlikely to address the problem adequately. One indication of this misplaced reliance is the fact that the Commission has not yet been able to enforce many of the existing rules on robocall mitigation. For example, multiple providers each year decline to respond to traceback requests, with no apparent consequences.⁴ Also, a close look at the Robocall Mitigation Database reveals that some—and possibly many—of the entries contain clear and serious compliance errors.⁵

³ See, e.g., Comments of EPIC and NCLC, *In re Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 (Jan. 10, 2022), <https://www.fcc.gov/ecfs/search/search-filings/filing/10111292652910>; Comments of ZipDX LLC, *In re Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 (Dec. 7, 2021); <https://www.fcc.gov/ecfs/search/search-filings/filing/12080110629539>; Comments of EPIC and NCLC, *In re Call Authentication Trust Anchor*, Notice and Request for Comment in WC Docket No. 17-97 (Nov. 12, 2021), <https://www.fcc.gov/ecfs/search/search-filings/filing/1113003014007>; Comments of EPIC and NCLC, *In re Numbering Policies for Modern Communications; Telephone Number Requirements for IP-Enabled Service Providers; Implementation of TRACED Act Section 6(a) Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket No. 13-97; WC Docket No. 07-243; WC Docket No. 20-67 (Oct. 14, 2021), <https://www.fcc.gov/ecfs/search/search-filings/filing/10153018018985>.

⁴ See note 1 *supra* at 21-22.

⁵ Just a few examples include the entries for the robocall mitigation plans certified by several providers. Humbolt VoIP and Huffman Telecom Corp. provide blank pieces of paper. VoIP Network, LLC provides a plan that is for another provider. And the plan for USATOLLNA.COM is the Commission’s instructions for filing on the database. See https://fccprod.servicenowservices.com/rmd?id=rmd_listings.

The Commission must recognize that currently there are insufficient inducements to counter the \$1 million in monthly revenue⁶ earned by complicit and complacent providers that transmit the one billion or more illegal calls made monthly.⁷ Under the current rules, the profit from these calls clearly makes it worthwhile for providers to run the risk of transmitting the calls. Yet the income to providers pales when compared to the approximately \$3 billion stolen every month from consumers through these fraudulent robocalls.⁸

This is the dynamic on which the Commission should focus. It must become more costly for providers to continue transmitting the calls than it is for them to not transmit them.⁹

⁶ By some estimates, robocallers can send one million calls for as cheaply as \$1,000 in call transmission costs; at a cost of \$0.001 per call, more than one billion scam robocalls every month means that providers earn more than \$1 million in revenue every month. *See, e.g.,* Comments of ZipDX LLC at 2, *In re Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 (Aug. 17, 2022), <https://www.fcc.gov/ecfs/search/search-filings/filing/108182676204994>.

⁷ Every month there are over 1 billion scam robocalls made to U.S. telephones, and a significant number of telemarketing calls. *See* PR Newswire, *Americans Hit by Just Under 46 Billion Robocalls in 2021, Says YouMail Robocall Index* (Jan. 6, 2022), <https://www.prnewswire.com/news-releases/us-phones-were-hit-by-more-than-50-billion-robocalls-in-2021-says-youmail-robocall-index-301455319.html> (21.4 billion scam calls in 2021, and 8.6 billion telemarketing calls). The distinction between the two appears to be somewhat fluid, as they depend on how the calls are classified. The universally-reviled calls selling auto warranties—recently targeted by the Ohio Attorney General and the Commission, *see* *Yost Files Suit Alleging Massive Robocall Scheme*, note 2 *supra*—are considered telemarketing calls, not outright scam calls. Conversation with Mike Rudolph, CTO, YouMail, Aug. 29, 2022.

⁸ In May 2022, HarrisPoll, in a survey commissioned by TrueCaller, estimated \$39.5 billion in consumer losses over the past twelve months. *See* TrueCaller, “TrueCaller Insights 2022 U.S. Spam & Scam Report” (2022), <https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report> (last visited Sept. 16, 2022). This is an average of more than \$3.29 billion in consumer losses per month.

⁹ Commissioner Starks has been beating this drum for some time. *See, e.g.,* *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) <https://docs.fcc.gov/public/attachments/FCC-21-105A3.pdf> (“As I have long said, illegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it.”).

III. Consumers Need Relief Now, and Tools Exist to Provide Relief Now

The Commission already has an effective tool that could be used to shut down scam robocalls by complicit providers. As we have proposed,¹⁰ the Commission should establish a more automated protocol for suspending serial violators from the Robocall Mitigation Database (RMD). Additionally, market pressure could be facilitated by encouraging the use of reputation scores,¹¹ or providing traceback transparency.¹² But the Commission's emphasis should first be on protecting subscribers from the scam calls. To meet the scale of the problem, an automated, systemized approach is necessary.

We encourage the Commission to offer specifics regarding what would trigger automated mitigation action (such as by suspending problem providers from the Robocall Mitigation Database).¹³ By whatever means the Commission chooses, it should implement a compulsory anti-robocall response on an expedited basis to eliminate—or at least meaningfully reduce—the billions of consumer fraud losses from these scam robocalls continuing to occur every month.

IV. Conclusion

We thank the Commission for the opportunity to comment on how it might better protect consumers from scam robocalls.

¹⁰ See note 1 *supra* at 14-27; NCLC and EPIC, Scam Robocalls: Telecom Providers Profit at 26-30 (June 2022), available at: <https://www.nclc.org/issues/energy-utilities-a-communications/scam-robocalls-will-continue-until-telecom-providers-no-longer-profit-from-them.html>.

¹¹ See, e.g., ZipDX Comments note 6 *supra* at 4-5; Reply Comments of Verizon at 9, *In re Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 (Jan. 10, 2022), <https://www.fcc.gov/ecfs/search/search-filings/filing/10110628206823>.

¹² See note 1 *supra* at 31-33.

¹³ Importantly, the Commission must not require that an identical call path be a prerequisite for any automated mitigation; we understand that traceback data, and signatures gathered by other tools, indicate that scam callers often diversify the providers through which they transmit their robocall traffic. See, e.g., ZipDX Comments note 6 *supra* at 4.

Respectfully submitted, this the 16th day of September 2022, by:

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

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