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**

Relating to the
Seventh Report and Order and Eighth Further Notice of Proposed Rulemaking
Issued May 19, 2023

Reply Comments of

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

By:

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

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

September 8, 2023

Table of Contents

Reply Comments

I. Summary and Introduction.

The **National Consumer Law Center** (NCLC), on behalf of its low-income clients, the **Electronic Privacy Information Center** (EPIC), and **Public Knowledge** file these comments on the Further Notice of Public Rulemaking (FNPRM) regarding "Advanced Methods to Target and Eliminate Unlawful Robocalls" issued on May 19, 2023.[1] We appreciate the Federal Communication Commission (Commission or FCC)'s continued efforts to address the problem of unlawful and unwanted robocalls, particularly several of the proposals included in this FNPRM. We support all of the proposals in this FNPRM, as they will assist in addressing the problem, especially if they are tweaked as we recommend.

However, as explained in **section II**, we do not believe the problem of scam and other illegal calls will be resolved even with full implementation of these proposals. To close the gap, we urge the Commission to consider a **market-based approach** as we describe, adding to the range of tools designed to protect subscribers from illegal calls.

In **section III,** we describe our support for the Commission's proposal to **require terminating providers to supply analytics-based call blocking to consumers on an opt-out basis**—as we believe that this proposal could make an important difference in the number of illegal, particularly scam, calls that are plaguing the telephones of American subscribers. We support requiring the implementation of reasonable Do-Not-Originate (DNO) lists. We also support empowering the Enforcement Bureau to direct providers to block traffic that is "substantially similar" to traffic they have been notified about and identify upstream providers, although we urge the Bureau to expand the grounds for blocking traffic.

Section IV describes our support for the Commission's proposed $11,000 base forfeiture, assuming it is a per day forfeiture.

---

[1] *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor, Seventh Report and Order, Eighth Further Notice of Proposed Rulemaking and Third Notice of Inquiry, CG Docket No. 17-59, WC Docket No. 17-97 (Rel. May 19, 2023), *available at* https://docs.fcc.gov/public/attachments/FCC-23-37A1.pdf [hereinafter FNPRM]. The Proposed Rule was published in the Federal Register at 88 Fed. Reg. 43,489 (July 10, 2023) and is available at https://www.federalregister.gov/documents/2023/07/10/2023-13032/advanced-methods-to-target-and-eliminate-unlawful-robocalls.

In **section V**, we support **call labeling** but caution that it is much less valuable to consumers than call blocking. We urge the Commission to not use labeling in lieu of blocking, but rather only when blocking is otherwise inappropriate.

Finally, in **section VI** we describe our support for the proposal to beef up the use of **reliable caller ID** in calls to wireless numbers, and we provide recommendations to ensure that the new system is reliable and trustworthy and does not exacerbate the use of fake caller IDs to scam victims.

II. The Commission should add a market-based approach to its arsenal.

Since the passage of the TRACED Act in 2019,[2] the Commission has implemented multiple initiatives to address the continuing onslaught of illegal calls.[3] However, despite this impressive list of creative undertakings, these dangerous, costly scam calls continue to plague American telephone subscribers at a staggering rate of more than one billion calls per month.[4] Those scam calls are in addition to more than one billion likely illegal telemarketing calls every month as well.[5]

We respectfully suggest that doing more of the same—requiring blocking of calls from FCC-identified providers, encouraging opt-out blocking and labeling, and enforcing and tweaking rules for STIR/SHAKEN authentication—seems unlikely to change the basic dynamic that drives these illegal calls: originating and gateway providers are making sufficient income from these calls to make it more profitable to keep making the calls and risking the punishment. Clearly the potential for costly consequences from conveying these illegal calls is sufficiently remote and outweighed by the income from these calls, such that the current measures fail to dissuade these providers from continuing their current practices.[6]

---

[2] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 (2019) (codified in 47 U.S.C. § 227b) (TRACED Act).

[3] *See* FNPRM at ¶¶ 6 through 64.

[4] YouMail estimates that 23% of 5.1 Billion robocalls in August were scams = 1.173 Billion scam robocalls. See YouMail Robocall Index, https://robocallindex.com/ (last visited Sept. 5, 2023).

[5] *See, e.g.*, National Consumer Law Center, Ex Parte, CG Docket No. 02-278, at 7-8 (filed Oct. 4, 2024), available at https://www.fcc.gov/ecfs/search/search-filings/filing/1005271665623.

[6] 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).

We urge the Commission to adopt a set of best practices for legal callers that—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 voice service providers who are currently complicit—either knowingly or with deliberate blindness—about their transmission of illegal calls. If legal callers were to demand on a uniform basis that the voice service providers of their calls must avoid transmitting illegal calls based on information uncovered by adopting these best practices, the profit from illegal calls would plummet.

The problems cited in this docket by legal callers illustrate that subscribers are not the only victims of the continuing onslaught of illegal calls. While subscribers are likely missing some calls that they want or need from callers,[7] legal callers are experiencing escalating costs and frustrations with consistently and reliably completing their calls to subscribers. These problems are caused by the mislabeling and incorrect blocking of their calls.[8]

Legal callers are responsible for placing over 2 billion robocalls every month. While there is not complete agreement on the degree to which subscribers want all of these calls (e.g., even legitimate calls from debt collectors may not always be wanted), there is no dispute that a significant percentage of these calls are desired, welcomed, or critical to their recipients (e.g., school, government, security, or disaster alerts). The difficulties with reliably completing these wanted calls is apparently increasing. Legal calls are mixed with a torrent of illegal calls at shared originating and intermediating providers, causing legal calls to be tainted by illegal calls in the same call path. The result is that legal calls end up mislabeled or blocked by downstream providers seeking to protect subscribers from illegal calls.

We are proposing that the Commission facilitate leveraging the considerable marketplace power of these legal callers to assist in the efforts to eliminate dangerous and unwanted calls—scam and illegal telemarketing calls. If legal callers are armed with the information about how to avoid using the providers that are processing illegal calls, the sheer economic power of legal callers may be sufficient to force voice providers to stop transmitting illegal calls.

---

[7] *See, e.g.*, Comments of Numeracle, Inc, WC Docket No. 17-97, CG Docket No. 17-59 at 2, 19 (filed Aug. 9, 2023), available at https://www.fcc.gov/ecfs/document/108102252803712/1.

[8] *Id.*

We suggest that the Commission define best practices for legal callers and provide clear recommendations to enable these callers to use their power in the telephone marketplace to ensure that their calls are only placed with providers that do not originate calls or transmit from illegal callers. A market-based approach like this would a) provide strong financial incentives to originating and intermediate providers to avoid transmitting illegal calls, b) facilitate the transmission of legal calls through call paths that would eliminate the likelihood that the calls 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 calls. **The foundation of a market-based approach is providing legal callers with the information that they need to keep their calls separate from illegal calls.** As we explain below, this information is already available from private analytics-based platforms, the Commission need only lead the way.

Legal calls are mistaken for illegal calls because of the lack of transparency regarding the providers that are transmitting both types of calls. As the Commission knows well, automated calls take circuitous routes from origination to the call recipient through the least-cost routing process.[9] The least-cost routing process allows downstream providers to refuse to take calls from upstream providers if they do not like the price offered for the transmittal or if they deem the calls potentially illegal—and thus too costly. The issue is how to incentivize downstream providers to refuse more of these illegal calls.

The phone network currently allows for legal calls to be mixed with illegal calls, which frustrates attempts to identify the illegal calls accurately and label or block them. Disaggregating legitimate calls from illegal traffic is the first step to resolving both problems. To do that, legal callers need to be equipped with the means to avoid the providers transmitting high volumes of illegal traffic alongside their legal calls.

The results of tracebacks and government investigations into illegal providers are only reported publicly after they are completed. To protect themselves, legal callers need to know in real time which providers are responsible for illegal calls, and they need to be made aware of how to use that information to protect their calls from being mislabeled or blocked.

---

[9] Appendix to Complaint, United States of America v. Palumbo, Case 1:20-cv-00473, Declaration of Marcy Ralston at 10-12 ¶ 22 (E.D.N.Y. Jan. 28, 2020), Marcy Ralston, a Special Agent in the Social Security Administration's Office of Inspector General, Office of Investigations, provided a sworn statement in *United States of America v. Palumbo.*

In their enforcement efforts, the Commission and other federal and state government agencies currently use information from non-government service providers that maintain real-time **content-based analytics** platforms. These platforms capture live evidence of illegal calls, including the content of the calls (both audio and transcribed), the telephone numbers of the callers and called parties, the date and time, the upstream voice service providers that provided STIR/SHAKEN attestation, and more. This information is aggregated to show volumes of calls, patterns in the calls, call paths, compliance with STIR/SHAKEN, and more. These content-based analytics platforms are also used by private enterprises in banking, healthcare, and hospitality and government agencies seeking to protect themselves from imposters. The platforms assist these institutions by identifying the voice service providers responsible for transmitting the imposter calls, facilitating the disruption of illegal calls.

There is no reason that legal callers could not use the information from these content-based analytics platforms to identify the providers responsible for transmitting illegal calls. Currently YouMail and ZipDX provide such services, and if this system were to be endorsed by the Commission, it is likely that more such operations would be launched.

Both of these platforms capture audio evidence and other material information on tens of thousands or millions of illegal calls daily. YouMail's solutions assist subscribers by identifying likely illegal calls, transferring those calls to voicemail, and then, with the permission of their consumers, capturing and transcribing the content of these calls. YouMail identifies the upstream providers and which providers applied the STIR/SHAKEN attestations to the calls. ZipDX performs similar functions using banks of its own telephone numbers (referred to as honeypots) to receive the calls. It also captures the audio content of the illegal calls and can determine the providers that originated or transmitted the illegal calls. Both platforms categorize and analyze the calls, providing extensive detail about call patterns and call paths as well as transcripts of the illegal calls. Both can also identify which telephone providers are continuing to provide STIR/SHAKEN attestations to illegal calls even after receiving notice of the bad traffic.

By using information from real-time content-based platforms, legal callers could identify which voice providers are continuing to process and transmit calls from sources of bad traffic. Once aware of which providers are participating in that conduct, a legal caller could switch to another originating provider that is not associated with illegal calls. Additionally, in its contracts with the providers originating their legal calls, the legal callers could require that the provider not send this

caller's traffic to immediately downstream providers that are transmitting illegal calls from upstream providers who are currently accepting bad traffic.

If sufficient numbers of legal callers employ these practices, in combination, considerable market pressure would be exerted on telecom providers to improve their mitigation efforts, as they would risk losing legal call traffic to competitors who are more effective at detecting and blocking bad traffic. Instead, at present, these originating and intermediate providers are rewarded when legal and illegal traffic are mixed together. That mixing masks illegal traffic, allowing the providers who are transmitting illegal traffic to continue profiting from it and further degrading the reliability of the American telephone system.

The Commission can provide information on best practices that would clarify for legal callers how to ensure that their calls are not mixed with the illegal calls. Once these best practices are adopted by legal callers, the Commission can provide additional requirements to downstream and terminating providers to step up their blocking of suspicious calls based on the feedback that they receive from their customers, providing further incentives to legal callers to ensure that their calls are sent on legitimate call paths. Callers will be incentivized to use this method because it will facilitate the delivery of their calls, but the Commission's expanded blocking requirements may provide an additional stimulus.

To prevent the telephone system from becoming further degraded by the prevalence of illegal, dangerous, and invasive calls, we urge the Commission consider recommending and facilitating these types of best practices for legal callers.

III. The Commission should implement its proposals for analytics-based blocking and delegating blocking authority to the Enforcement Bureau but should expand the basis upon which the Bureau initiates blocking.

Consumers will benefit from the Commission's proposals to require analytics-based blocking and blocking based on Do-Not-Originate (DNO) lists and the proposal to delegate blocking authority to the Enforcement Bureau. As such, we support these proposals.

We support the Commission's proposal to require analytics-based blocking of calls that are highly likely to be illegal, provided to consumers on an opt-out basis.[10] As the Commission notes,[11]

[10] *Id.* at ¶¶ 71-75.

[11] *Id.* at ¶ 73.

opt-out is preferable to opt-in, as opt-out does not put a burden on consumers to be aware of the option, to communicate their preference, and to confirm that their preference has been honored.

We also support the Commission's proposal to require blocking based on a reasonable DNO list.[12] We urge the Commission to articulate what enforcement measures a provider should expect to face if it fails to implement a reasonable DNO list.

Additionally, we support the Commission's proposal to authorize the Enforcement Bureau to require blocking where a provider has received a Notice of Suspected Illegal Traffic and continues to receive traffic substantially similar to the traffic identified in the Notice.[13]

However, we urge the Commission to enlarge the criteria used to determine whether a provider is intentionally or negligently allowing illegal traffic onto its network.[14] The criteria should **include providers who were the recipients of either a) Civil Investigative Demands (CIDs) from state or federal enforcement officials or b) notices or inquiries from other trusted third parties certified by the FCC or other enforcement officials to provide these services.**

IV. The Commission should implement its proposed base forfeiture, assuming the forfeiture applies daily.

Assuming the forfeiture would apply for every day that a provider fails in its duties, we support the Commission's proposal for a base forfeiture of $11,000 for failing to take affirmative, effective measures to prevent new and renewing customers from using the provider's network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its service is not used to originate illegal traffic.[15] We also support the Commission's proposal to authorize the forfeiture to be increased to the maximum allowed.[16]

---

[12] *Id.* at ¶¶ 76-79.

[13] *Id.* at ¶¶ 80-89.

[14] *Id.* at ¶ 88.

[15] *Id.* at ¶101 (citing to 47 CFR § 64.1200(n)(3).

[16] *Id.* (citing to 47 CFR § 1.80(b)(9); see also 47 U.S.C. § 503(b)(2)(D)).

V. Call labelling should be used only when call blocking is clearly not appropriate.

Calls that are highly likely to be scam or other illegal calls should be blocked. Providers should not be permitted to take the less rigorous path of labeling calls instead of blocking them if they could otherwise determine that a call is likely to be illegal. Illegal calls—especially those that perpetrate scams—present real danger to consumers, and the providers are in a much better position than the consumers to assess the risk of each particular call. There are extensive call tracking systems developed in the telecommunications ecosystem today that easily identify the content of repeated calls—illustrating the degree of danger that the calls pose to recipients—as well as the source and recipients of these calls and the numbers of the calls.[17] Terminating providers should be encouraged to block calls, rather than simply label them, based on information from these service providers.

Call labeling should only be used in lieu of blocking when there is meaningful doubt about the legality and value of the call, such that allowing the call to go through poses less risk than blocking it. In other words, calls that appear to be likely scams should always be blocked, as the risk to consumers from those calls is significant. Truecaller's survey data indicates that over 68 million people in the United States fell victim to call scams in 2022, losing over $39 billion to scammers.[18] At the same time, losses **reported** to the FTC rose to $802 million.[19] Blocking of these calls should be the first and primary line of defense, not labeling.

VI. Reliable caller-ID capacity should be added to wireless lines only with assurances that it provides meaningful information.

We support the Commission's proposal to beef up the use of **reliable caller ID** in calls to wireless numbers, and we understand that the use of Rich Call Data to display Caller Names is the best way forward to implement that system.

---

[17] YouMail confidential data provided to NCLC.

[18] *See* Truecaller, Truecaller Insights 2022 U.S. Spam and Scam Report (May 24, 2022), https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report.

[19] *See* FTC Consumer Sentinel Network, Fraud Reports by Contact Method, Reports & Amount Lost by Contact Method (Losses & Contact Method tab, with quarters 1 through 4 checked for 2022), *available at* https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts.

We have some concerns, however, regarding tying the use of this new system to A-level attestation if the Commission continues to permit the use of rented DIDs. As we have explained,[20] some VoIP providers advertise the use of rented DIDs just for the purpose of allowing callers to pretend to be someone other than themselves **for the express purpose of evading blocking and labeling efforts.**[21] A-level attestations are attached to these calls, even though the numbers only belong to the caller for a small amount of time and the display of the telephone number provides no meaningful information to either the downstream providers or the recipients of the calls. Scam and other illegal callers can circumvent STIR/SHAKEN by cycling through reams of disposable numbers. This completely undermines the entire purpose of the STIR/SHAKEN system.

Adding a name to the call which is not the real name of the caller will only facilitate more illegal calls rather than decreasing them. The A-level attestation is not a meaningful certification of the reliability of the caller ID attached to calls. And if scammers are permitted to add fake caller ID names to their scam calls, more people will be tricked into answering these calls and becoming victims of scams. We are concerned that until the problem of rented DIDs is resolved, building on the current unreliable system may not be prudent. We note also that USTelecom agrees the Commission should address "how bad actors are obtaining access to real numbers, including through number rental."[22]

Conclusion.

We appreciate the Commission's consideration of our proposals and concerns. We would be happy to answer any questions.

---

[20] *See, e.g.*, Comments of National Consumer Law Center and Electronic Privacy Information Center, WC Docket No. 17-97 (filed June 5, 2023), available at https://www.fcc.gov/ecfs/document/10605050535175/1 [hereinafter NCLC/EPIC 6FNPRM Comments].

[21] *See, e.g.*, Luke Genoyer, What is a Dynamic Caller ID for VoIP?, United World Telecom blog (June 23, 2020), https://www.unitedworldtelecom.com/learn/what-is-a-dynamic-caller-id-for-voip/, ("Is it possible to change an outgoing caller ID? Yes, **with the VoIP feature, dynamic caller ID, your business can display a local or toll-free number instead of a long-distance or international number**.") (emphasis added) (last visited September 5, 2023).

[22] Comments of USTelecom – The Broadband Association, WC Docket No. 17-97, at 3 n.13 (filed July 5, 2022), available at https://www.fcc.gov/ecfs/search/search-filings/filing/1070508154864 (citing to NCLC/EPIC 6FNPRM Comments at 1, 4; Comments of USTelecom – The Broadband Association, CG Docket No. 17-59, WC Docket No. 17-97, at 13-14 (filed Aug. 17, 2022)).

Respectfully submitted by:

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

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

September 8, 2023