Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

COMMENTS ON THE NOTICE AND REQUEST FOR COMMENTS

by

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

Submitted November 12, 2021

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

Summary

We applaud the Commission's proposal regarding reducing the extension granted to small voice service providers to comply with the STIR/SHAKEN protocol from two years to one year. As the Commission has recognized in its request for comments, the timeline for compliance needs to be shortened. We strongly support this change. But, even more importantly, we urge the Commission to use as the basis of determining which providers should qualify for a continuing extension or any extension in the future the actual compliance record of each provider.

The ongoing plague of fraudulent robocalls that are still bombarding our telephone lines necessitates that the Commission take an aggressive response in regulating the providers that are bad actors.

A single scammer, along with complicit downstream carriers, can still dump millions of calls to consumers within a single month, annoying all who receive these calls, terrifying some who listen to these scam calls, and costing many of these consumers thousands of dollars—or more. The intermediate providers who accept calls from the originating or gateway providers claim that they cannot adequately police traffic on their networks. But such proclamations of innocence are hard to believe, as those providers continue to allow upstream providers access to their networks despite their direct knowledge of multiple traceback requests about calls coming from those bad actor providers.

As the Commission decides what categories of providers should be denied a continued extension, it should use the compliance-based methodology it has already articulated to determine the extent to which it will continue to recognize a coming-into-compliance grace period. Where a provider has been non-compliant, that provider should be removed from the Robocall Mitigation Database. While non-compliance should be an obvious trigger for escalated enforcement, we urge the Commission to also employ a constructive notice-based methodology.

None of the alternative methodologies suggested by commenters are as effective at targeting non-compliant providers. An approach based solely on call volume could unfairly capture large-

volume small voice providers who have been compliant and have demonstrated no deficiency in their monitoring and responding as part of their robocall mitigation program. If the problem is illegal robocalls, the solution should be based on who is perpetrating *illegal* robocalls, not who is perpetrating a high volume of calls generally.

Similarly, while many commenters have advocated for a facilities-based methodology—reasoning that illegal robocalls are rarely associated with facilities-based providers—this would unfairly capture non-facilities-based providers who have otherwise been compliant and have demonstrated no deficiency in their monitoring and responding as part of their robocall mitigation program. And, applying an arbitrary factor such as whether a provider has facilities undermines incentives for non-facilities-based providers to comply with the rules and align their business practices with the goal of facilitating only legitimate calls.

Table of Contents

Comments

I. Introduction

The Federal Communications Commission (Commission or FCC) issued a Notice and Request for Comment[1] requesting comment on the issue of whether extensions granted by the Commission to some voice service providers in implementing the STIR/SHAKEN protocol should be shortened. The **Electronic Privacy Information Center (EPIC)**,[2] and the **National Consumer Law Center**[3] **(NCLC)** on behalf of its low-income clients, appreciate the opportunity to file these comments to encourage the Commission to modify in several material ways the extension provided to small voice service providers in achieving compliance with the protocol. As the Commission has recognized in its request for comments, the timeline for compliance needs to

[1] See Federal Communications Commission, Call Authentication Trust Anchor, Notice and Request for Comment, WC Docket No. 17-97, DA Docket No. 21-1103, 86 Fed. Reg. 50,347 (Oct. 12, 2021) [hereinafter Request for Comment], *available at*: https://www.federalregister.gov/documents/2021/10/12/2021-22106/call-authentication-trust-anchor

[2] EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC routinely files amicus briefs in TCPA cases, has participated in legislative and regulatory processes concerning the TCPA, and has a particular interest in protecting consumers from robocallers. *See, e.g.,* Br. of Amici Curiae Electronic Privacy Information Center (EPIC) and Twenty-Two Technical Experts and Legal Scholars in Support of Respondent, Facebook v. Duguid, 141 S. Ct. 1163 (2020) (No. 19-511); Br. for EPIC et al. as Amici Curiae Supporting Petitioner, Barr v. Am. Ass'n of Political Consultants, Inc., 140 S. Ct. 2335 (2020) (No. 19-631); EPIC Statement to House Energy & Commerce Committee, Legislating to Stop the Onslaught of Annoying Robocalls, April 29, 2019.

[3] 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 and the U.S. Supreme Court, 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*, Chapter 6 (3d ed. 2017), updated at *www.nclc.org/library*.

be shortened. But, even more importantly, the determination of which providers should qualify for any extension in the future should be based primarily on the compliance record of each provider.

Because of the ongoing plague of fraudulent robocalls that are still bombarding our telephone lines, we urge the Commission to take an aggressive response in regulating the providers that are bad actors. First, the Commission should only permit extensions to providers who have a history of strict compliance with all of the Commission's requirements, including immediate response to any appropriate notice (such as from the Industry Traceback Group (ITG)),[4] the Commission, or other enforcement efforts). Second, the Commission should compel participation in a more robust monitoring regime of providers who are dumping the dangerous calls into the American telephone network and impose penalties on providers who transmit these providers' calls.

Congress has explicitly stated that the purpose of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act is to protect consumers,[5] and there is no good reason that the Commission cannot act now to stop these calls from continuing.

At this time--almost two years after the TRACED Act was passed[6]--a single scammer along with a system of complicit carriers can still place millions of calls to consumers within a single

---

[4] The Commission was required by the TRACED Act to issue rules "for the registration of a single consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls." *In re* Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), Report and Order, EB Docket No. 20-22, at ¶ 1, *available at* https://docs.fcc.gov/public/attachments/DA-21-1047A1.pdf. On July 27, 2020, the Enforcement Bureau selected USTelecom's Industry Traceback Group (ITG) to serve as the registered consortium. Id. at ¶ 4. On August 25, 2021, the Enforcement Bureau once again selected ITG to serve as the registered consortium for tracing back suspected illegal robocalls. Id. at ¶ 1.

[5] Six Senate and House leaders said at the TRACED Act's passage: "It's time to put Americans back in charge of their phones." https://energycommerce.house.gov/newsroom/press-releases/house-senate-announce-agreement-on-anti-robocall-bill Sen. Markey said "The daily deluge of robocalls that Americans experience is more than a nuisance, it is a consumer protection crisis. Today, the Senate is telling robocallers that their days are numbered." https://www.thune.senate.gov/public/index.cfm/press-releases?ID=E4F86936-0419-48FB-BCD6-EC05CC71FE60

[6] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (Dec. 30, 2019) [hereinafter TRACED Act].

month, annoying all who receive these calls, terrifying some who listen to these scam calls, and costing many of these consumers thousands of dollars—or more. As described in Section II *infra*, the intermediate providers who accept calls from the originating or gateway providers claim that they cannot adequately police traffic on their networks. But such proclamations of innocence are hard to believe, as those providers continue to allow upstream providers access to their networks despite their direct knowledge of multiple traceback requests about calls coming from the bad actor providers.

However, if the Commission were to make a determination about continuing extensions based on factors that fail to take in to account a provider's actual diligence in responding to evidence of upstream bad actors (what a provider does in response to what it knows or should have known) as well as that provider's compliance overall, the Commission would be undermining its own goal to mitigate robocalls. For example, basing an extension on whether a provider has facilities would frustrate incentives for non-facilities-based providers to comply with the rules and align their business practices with the goal of facilitating only legitimate calls.

II. The Ongoing Massive Consumer Harms from Robocalls Demonstrate that the FCC Must Act Quickly.

Recent enforcement efforts of many state Attorneys General, cases filed in numerous federal courts through the country, and the actions taken by this Commission and its sister agency, the Federal Trade Commission, should thoroughly illustrate the need to aggressively combat illegal calls. Fraudulent, deceptive, scam callers initiating calls from within the U.S. and outside the U.S. are reaching American consumers millions of times a day.[7] These calls are annoying to many of us. But some callers are **defrauding** the least sophisticated and the most vulnerable consumers by scaring

[7] In the first ten months of 2021, YouMail estimates that Americans received nearly 43 billion robocalls. This is an increase of more than four billion robocalls over this same time period last year. YouMail, *Historical Robocalls by Time*, https://robocallindex.com/history/time (last visited Nov. 12, 2021).

them into turning over money most of these consumers cannot afford to pay. A single bad actor or continuum of bad actors is often responsible for millions of illegal scam calls. The Commission itself has estimated that these scam calls costs Americans $10 billion annually.[8]

The following are just a few examples of a significant and growing problem impacting Americans—all because scam callers are permitted access to the nation's telephone system:

1. In the first nine months of 2021 alone, South Carolina consumers collectively lost nearly half a million dollars to illegal robocalls,[9] despite the partial implementation of STIR/SHAKEN.[10]
2. Since 2020, one system of providers (Startel, Piratel, VoIP Essential[11]) has facilitated millions of robocalls to residents the State of Indiana,[12] and tens of millions of calls nationwide.[13] Originating and intermediate providers continued to process these calls to subscribers even after nine traceback requests from USTelecom were sent to Startel in 2020-2021.[14] For example, despite receiving four traceback requests in the

[8] FCC, "FCC Mandates That Phone Companies Implement Caller ID Authentication to Combat Spoofed Robocalls" at 1 (March 31, 2020), *available at* https://docs.fcc.gov/public/attachments/DOC-363399A1.pdf.

[9] $493,670. South Carolina Department of Consumer Affairs (SCDCA), Comment on Numbering Policies for Modern Communications, WC Docket Nos. 13-97, 07-243, 20-67 (Oct. 14, 2021) at 2, https://ecfsapi.fcc.gov/file/1014212236856/FCC%20VoIP%20Numbering%20Policies%20-%20SCDCA%20Comment%20Letter%20-%20final%20submitted.pdf.

[10] SCDCA also notes that "The continuing trend of monetary losses reported by consumers receiving unsolicited calls even after implementation of STIR/SHAKEN, comprised of potential and actual losses, also supports adding more protections." Id. at 3.

[11] Plaintiff's Complaint for Civil Penalties, Permanent Injunction, Other Equitable Relief, and Demand for Jury Trial, Indiana v. Startel Communication LLC, No. 3:21-cv-00150-RLY-MPB, 2021 WL 4803899 at ¶ 6, 15, 18, 47, 58 (S.D.Ind. Oct. 14, 2021).

[12] Id. at 39-41, 50-53, 62-65, 573; indeed, according to an Indiana news services some subscribers were receiving 25 robocalls a day. Angela Brauer, "Hoosiers share frustration over incessant robocalls & scam text messages," CBS4Indy (Oct. 13, 2021), *available at* https://cbs4indy.com/investigations/indiana-robocalls-scam-text-messages/.

[13] Compl., Startel, 2021 WL 4803899 at ¶ 124.

[14] Id. at ¶ 247.

prior three weeks, in July 2020, Piratel continued carrying Startel's traffic.[15] Startel continued processing these calls through its network, even after July 2020, when the ITG offered suggestions to Startel to prevent illegal calls.[16] At some point in 2020, Piratel suspended Startel[17] but this suspension did not last.[18] In February 2021, more than six months after ITG made suggestions to Startel about how to monitor and reduce its illegal traffice, when Piratel informed Startel that IRS or SSA scam calls were coming through its network, Startel claimed that it had did not know how this could have happened: "we monitor maximum calls very carefully. But what exactly happened is still unknown to us…"[19] Six months after that, in August 2021, Piratel emailed Startel requesting additional information about Startel's robocall mitigation procedures.[20] As of October 2021, Startel had not replied with the requested information, yet Piratel continued to carry Startel's traffic.[21] Even knowing about multiple tracebacks of its upstream provider (i.e. Startel), Piratel continued to carry Startel's traffic.[22] VoIP Essential was also warned multiple times that Startel was sending illegal robocall traffic, but VoIP Essential continued to carry Startel's traffic.[23] As of the time of these comments, Piratel and VoIP Essential are both still

[15] Id. at ¶ 314, 316.

[16] Id. at ¶ 311.

[17] Id. at ¶ 384.

[18] Id. at ¶ 387.

[19] Id. at ¶ 415.

[20] Id. at ¶ 431.

[21] Id. at ¶ 432, 437-38.

[22] Id. at ¶ 247-48, 258-59, 283-84, 291-92, 325-26.

[23] Id. at ¶ 565.

listed in the Robocall Mitigation Database; VoIP Essential requested an extension as a small voice services provider.[24]

3. In 2019, one single intermediary VoIP provider[25] facilitated *hundreds of millions* of calls within 23 days,[26] depriving consumers of "substantial sum[s]"[27] totaling in the hundreds of thousands of dollars,[28] and costing at least one 84-year old consumer approximately $10,000 because the caller impersonated the U.S. Marshals Service and scared the consumer into paying this amount.[29] Yet, this provider knew full well that it was processing illegal and dangerous calls, because between May 2019 and January 2020, this provider had received 66 traceback notifications from USTelecom.[30] And, since 2017, it had received no fewer than 100 separate notifications of fraudulent activity.[31] Yet this provider, TollFreeDeals.com, alleged in federal court that it was impossible for it, as a carrier, to respond and stop fraudulent traffic on its network.[32]

---

[24] VoIP Essential is listed as Rapid Eagle Inc., with FCC Registration Number (FRN) 0029292232; Piratel's FRN is 0021441233. Federal Communications Commission, Robocall Mitigation Database, https://fccprod.servicenowservices.com/rmd?id=rmd_listings (last accessed Nov. 12, 2021). In February 2020, the Commission requested Piratel's assistance with a traceback request for foreign-originated Social Security scam robocalls. Letter to Piratel from Rosemary E. Harold, Chief, Enforcement Bureau, FCC (Feb. 4, 2020), *available at* https://docs.fcc.gov/public/attachments/DOC-362256A1.pdf Startel's illegal robocalls included Social Security scam calls. Compl., Startel at ¶ 26.

[25] Action for Temporary Restraining Order, United States v. Palumbo, 20-cv-00473-ERK-RLM (Jan. 28, 2020), *available at* https://www.justice.gov/opa/press-release/file/1240026/download.

[26] Department of Justice, The Department of Justice Files Actions to Stop Telecom Carriers Who Facilitated Hundreds of Millions of Fraudulent Robocalls to American Consumers (Jan. 28, 2020), *available at* https://www.justice.gov/opa/pr/department-justice-files-actions-stop-telecom-carriers-who-facilitated-hundreds-millions.

[27] United States v. Palumbo, 448 F. Supp. 3d 257, 259 (E.D.N.Y. 2020).

[28] No less than $130,250. United States v. Palumbo, 448 F. Supp. 3d 257, 264 (E.D.N.Y. 2020).

[29] "J.K. lost $9,800 to this scam." United States v. Palumbo, 448 F. Supp. 3d 257, 262 (E.D.N.Y. 2020).

[30] United States v. Palumbo, 448 F. Supp. 3d 257, 261 (E.D.N.Y. 2020).

[31] United States v. Palumbo, 448 F. Supp. 3d 257, 261 (E.D.N.Y. 2020).

[32] United States v. Palumbo, 448 F. Supp. 3d 257, 266 (E.D.N.Y. 2020).

4. In just one nationwide scam robocall campaign pretending to sell magazine subscriptions, the scammers tricked thousands of consumers into paying $300 million. One Minnesota woman began paying $24 per month for magazines and soon found herself being charged $64 multiple times per month. When she confronted the scammers, they told her if she paid $1,000, they would go away. Many other victims were elderly, and some were charged as much as $1,500 per month.[33]

These are but a few examples of the magnitude of harm an originating provider can facilitate by allowing a single bad actor to make calls through its network. As described above, in less than one month's time, one such provider can be responsible for millions of harmful calls. And because of the tracebacks conducted by USTelecom, **the FCC knows the identities of the responsible providers**: they are the subject of one or more traceback requests for their callers.

A single traceback request from USTelecom is itself notice to the providers that they are carrying illegal calls. Multiple requests should be considered equivalent to a neon sign flashing "Warning, Warning" to the providers who originated the calls, and to those who transmitted the calls from the originating or gateway provider.

As of its Fourth Report and Order, the Commission required voice providers to effectively mitigate illegal traffic when notified by the Commission.[34] Yet, the FCC has not prohibited providers—either as originating or intermediate providers— from continuing to transmit calls from

[33] Lauren Leamanczyk, "Inside one of Minnesota's biggest phone scams," KARE11 News (May 12, 2021), *available at* https://www.kare11.com/article/news/investigations/robocalls/inside-one-of-minnesotas-biggest-phone-scams/89-52807423-0f38-492d-853a-98e52827d3b0.

[34] *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls, Fourth Report and Order, CG Docket No. 17-59, at ¶ 23-25, *available at* https://docs.fcc.gov/public/attachments/FCC-20-187A1.pdf. [Fourth Report]

bad actors through their systems. Instead, the Commission has only *allowed* providers to stop transmitting the calls, after notice to the FCC.[35] This is wrong.

Congress explicitly empowered the FCC to stop these illegal calls. When it comes to balancing the relative rights and needs of consumers who need to be protected from these dangerous and unmistakably fraudulent calls, against the "rights" of those providers who conveniently ignore repeated warnings and other signs of the consequences of their business decisions, the outcome should be clear. The FCC should not give the benefit of the doubt to the very businesses that are profiting from the harassment and defrauding of American telephone subscribers. The Commission is failing to protect subscribers, even though it has the means, and the clear mandate from Congress to do so.

III. The Commission Should Grant Extensions Based on Whether Providers Have Demonstrated Compliance and Effective, Affirmative Mitigation Measures.

The Commission's October 1, 2020 order permits providers to supply confidential certifications of the efforts they will be undertaking to mitigate illegal robocalling passing through their networks.[36] However, the robocall scourge persists, often over small voice service provider networks. The Commission is now considering a different approach—modifying the extension it granted to small voice service providers. We agree with this proposal, and we urge the Commission to use its existing authority to reduce the extensions from two years to one year to comply with STIR/SHAKEN.

---

[35] Id. at ¶ 6, 8, 30.

[36] *In re* Call Authentication Trust Anchor, Second Report and Order, WC Docket No. 17-97, at ¶ 83, 122-23, *available at* https://www.fcc.gov/document/fcc-adopts-new-rules-combat-spoofed-robocalls-0. [Second Order]

However, we urge the Commission to use as the criteria to deny ongoing extensions if the provider failed to comply with the STIR/SHAKEN requirements or had constructive notice that it was processing illegal calls (i.e. whether the provider "knew or should have known" they were trafficking illegal robocalls on their networks). Alternative methods, such as those based on trends suggesting that facilities-based providers are least responsible for the harm, lump the good in with the bad, failing to distinguish between compliant providers and bad actors. Those alternatives also do not create incentives for compliance for the small providers.

A. The Commission Should Apply a Compliance-Based Methodology in Evaluating Whether to Grant an Extension.

Both the TRACED Act and the previous Commission rulings have already established the appropriate basis for a fair determination of which providers should be entitled to the extension: the Commission should leverage its own explicit requirements and standards that have already been imposed on providers. Now, as the Commission decides the standards to determine which of providers should be denied a continued extension, it should use the compliance-based methodology it has already articulated to determine the extent to which it will continue to recognize a coming-into-compliance grace period.

In its Third Further Notice of Proposed Rulemaking (3NPR), the Commission required voice service providers seeking an extension to implement a robocall mitigation program, comply with requirements to respond fully and in a timely manner to traceback requests, mitigate illegal traffic when notified by the Commission, and "adopt affirmative, effective measures to prevent new and renewing customers from using their networks to originate illegal calls."[37] By now, a provider's

[37] 3NPR at ¶ 4 (citing to 47 CFR § 64.1200(n)(3); see also Call Blocking Fourth Report and Order, 35 FCC Rcd at 15229-30, 32, at ¶ 22, 32).

failure to meet any of these criteria should result in loss of the extension. For example, ZipDX LLC has proposed that a history of no illegal call tracebacks and no warning letters be required for any extension.[38] These seem logical as indicators of good faith efforts and effective measures towards mitigating illegal robocalls. By this methodology, Piratel would have been denied an extension as of February 2020, if not earlier.[39] Instead, approximately 10 million calls from Startel alone passed through Piratel's network between January and July 2020.[40]

Also, in its Fourth Report and Order under Docket 17-59, Advanced Methods to Target and Eliminate Unlawful Robocalls, the Commission required voice providers of all sizes to implement effective measures to prevent new and renewing customers from originating illegal calls, such as imposing and enforcing relevant contract terms.[41] When evaluating whether a given small voice service provider is entitled to a continuing extension, the Commission should assess the extent to which that provider has complied with the Fourth Report and Order.

Where a provider has been non-compliant, that provider should be removed from the Robocall Mitigation Database. Examples of non-compliance can be found in the bulleted list in Section IV, *infra*. To this list, we would add that a provider who has been the subject of more than one traceback request should also be considered non-compliant.

The Commission has noted that it cannot reduce the extension granted to entities that rely on a non-IP network to comply with STIR/SHAKEN protocols,[42] but this does not impair the Commission's ability to determine a mitigation program offered by one of these providers to be

---

[38] *See* Comments of ZipDX LLC, WC Docket No. 17-97, at 2 (filed July 26, 2021), *available* https://ecfsapi.fcc.gov/file/10726649603037/ZipDX-17-97-3rdFNPRMReply.pdf.

[39] Harold Letter, *supra* note 24.

[40] Startel placed 9,934,413 calls through Piratel's network between January 1, 2020 and July 21, 2020. Comp., Startel, at ¶ 316, 374.

[41] Fourth Report at ¶ 35, Appendix C, ¶ 9.

[42] 3NPR at ¶ 19.

insufficient. This approach, and the authority on which it is based, is generally discussed in Section IV, *infra*.

B. The Commission Should Also Apply a Constructive Notice-Based Methodology in Evaluating Whether to Grant an Extension.

Enforcement based on non-compliance is a good start to combatting robocalls; but the Commission should also consider where its current requirements may be appropriately supplemented. While non-compliance should be an obvious trigger for escalated enforcement, we urge the Commission to also employ a constructive notice-based methodology (i.e. an approach based on whether the provider "knew or should have known" their networks were being used to transmit illegal robocalls). Providers could be adhering to everything that they certified that they would do and technically fall within the parameters of the Commission's standards-based approach to enforcement (e.g. "reasonable measures"), yet still willfully ignore clear indicators that they are responsible for illegal robocall traffic reaching consumers.

In its 3NPR, the Commission proposed defining a subset of small voice service providers as those "most likely to originate a significant quantity of unlawful robocalls."[43] As we noted in Sections II and III of our comments on the further notice of proposed rulemaking in Docket 13-97, Numbering Policies for Modern Communications, the Commission should also articulate specific data points that are indicative of illegal robocalling activity, and hold providers accountable for monitoring for these data points on their networks and for responding appropriately.[44] In short, providers should monitor call characteristics (e.g. frequency and/or duration of calls), caller

[43] 3NPR at ¶ 20.

[44] *See* Comments of EPIC and NCLC, WC Docket Nos. 13-97, 07-243, 20-67, at 3-10 (filed Oct. 14, 2021), *available at* https://ecfsapi.fcc.gov/file/10153018018985/EPIC%20NCLC%20Number%20Policies%20Comment_21-10-14_CF.pdf.

characteristics (e.g. rate at which number bank is refreshed), and compliance characteristics (e.g. volume of complaints, strength of provider's robocall mitigation plan).[45] Similar data points should form the elements of a constructive notice-based methodology, by which the Commission determines the likelihood of a provider to originate a significant volume of unlawful robocalls based on the provider's diligence—or negligence—in monitoring and responding to relevant indicators, and thereby determines whether to grant a continuing extension.

C. None of the Alternative Methodologies Suggested by Commentors are as Effective at Targeting Non-Compliant Providers.

In its Notice and Request for Comment, the Commission proposed making determinations about extensions based on call volume or other characteristics like provision of mass-market services[46] or the number of subscriber lines.[47]

While it is logical to escalate enforcement against providers who currently have the greatest call volume, this does not directly deal with the actual problem the Commission has been tasked with addressing. An approach based solely on call volume could unfairly capture large-volume small voice providers who have been compliant and have demonstrated no deficiency in their monitoring and responding as part of their robocall mitigation program. If the problem is illegal robocalls, the solution should be based on who is perpetrating *illegal* robocalls, not who is perpetrating a high volume of calls generally.

---

[45] Id. at 9.

[46] 3NPR at ¶ 6, 22-29.

[47] Counting number of subscriber lines is particularly unlikely to be effective, as some platforms allow an entity to reach "hundreds of thousands" of consumers in a single day without using a high volume of subscriber lines. *See* Comments of USTelecom, WC Docket No. 17-97, at 2 (filed July 9, 2021), *available at* https://ecfsapi.fcc.gov/file/1070908863075/USTelecom%20-%20Comments%20re%20Small%20Provider%20STIR-SHAKEN%20Extension%20FINAL.pdf.

Similarly, while many commenters have advocated for a facilities-based methodology[48]—reasoning that illegal robocalls are rarely associated with facilities-based providers—this would unfairly capture non-facilities-based providers who have otherwise been compliant and have demonstrated no deficiency in their monitoring and responding as part of their robocall mitigation program. And, applying an arbitrary factor such as whether a provider has facilities undermines incentives for non-facilities-based providers to comply with the rules and align their business practices with the goal of facilitating only legitimate calls.[49] Moreover, this approach fails to account for whether an entity is acting in good faith.

However, if the Commission decides to apply a facilities-based methodology, the FCC should prevent abuse of that system by evaluating on a services-by-services basis rather than on an entity-by-entity basis. This is similar to how the Commission defined voice services,[50] and it also addresses a recurring Commission concern regarding entities gaming its classification systems.[51]

By evaluating "facilities-based" at an entity level, the Commission would be permitting—for example— a provider to pass 1% of its traffic through a facility it leased or owned and thereby grant an extension covering the 99% of the provider's traffic that is not actually facilities-based. If instead the Commission evaluates "facilities-based" at a services level, only those services which are facilities-based would be granted the extension. We reiterate that even a services-level evaluation of

---

[48] *See e.g.*, Comments of ACA Connects, WC Docket No. 17-97, at 10 (filed July 9, 2021), *available at* https://ecfsapi.fcc.gov/file/10709401808700/210709%20-%20ACA%20Connects%20Comments%20on%20STIR-SHAKEN%20Third%20Further%20Notice.pdf.

[49] Whether a provider is facilities based or not might be an appropriate factor on which the Commission might prioritize which providers should be scrutinized first: allowing facilities-based providers to enjoy a short continuation of the extension while the Commission determines their compliance.

[50] Second Order at ¶ 23 (utilizing a call-by-call determination of "voice services" not an entity-by-entity determination).

[51] *See e.g.,* 3NPR at ¶ 32 "How should we prevent voice service providers from gaming such a definition by retaining a small TDM network or a TDM network element?"

facilities-based providers fails to account for whether that provider is responsive to indicators that upstream providers are using its network to pump illegal robocalls to American consumers.

Bad actors like Startel and Piratel have shown that they cannot be trusted to meaningfully comply with the TRACED Act on their own, and so the Federal Communications Commission must use the tools it already has at the ready, such as de-listing from the Robocall Mitigation Database, to compel providers to implement effective robocall mitigation programs. The Commission should immediately begin with non-compliant providers and expand to include providers who "knew or should have known" that they were responsible for facilitating illegal robocalls.

IV. The Commission Should Take Action Against Providers with Insufficient Robocall Mitigation Programs

In this Request for Comment, the Commission has proposed reducing the extension it granted to small voice service providers. As explained, we support this reduction, but we also urge the Commission to explicitly follow the mandates of Section 4 of the TRACED Act, which requires it to identify small voice providers whose compliance date has been extended but who are "repeatedly originating large-scale unlawful robocall campaigns," and require them "to take action to ensure that such provider does not continue to originate such calls."[52] Congress also explicitly instructed the Commission to "take reasonable measures to . . . enable as promptly as reasonable full participation of all classes of providers . . . to receive the highest level of trust."[53] These measures

[52] TRACED Act § 4(b)((4)(C)(ii).

[53] TRACED Act § 4(b)(4)(D).

explicitly include "limiting or terminating a delay of compliance if the Commission determines . . . that the provider is not making reasonable efforts to develop the call authentication protocol . . . ."[54]

Section 4 of the TRACED Act requires voice service providers to implement the STIR/SHAKEN framework on the IP portion of their networks and "take reasonable measures to implement an effective call authentication framework" in the non-IP portion of their networks by June 30, 2021.[55] In its Second Order, the Commission provided an extension to small voice providers, and made it contingent upon implementing an *effective* robocall mitigation program and filing a certification with the FCC "showing how they are acting to stem the origination of illegal robocalls."[56] Most importantly, the Commission noted that a provider must comply with its stated mitigation program or else the program will be deemed insufficient, and that the Commission "will also consider a mitigation program insufficient if a provider knowingly or through negligence serves as the originator for unlawful robocall campaigns."[57]

That same order stated that enforcement responses to deficient submissions would include removal from the Robocall Mitigation Database after providing an opportunity to cure, requiring the submission of more specific requirements, and imposition of forfeiture.[58] As of September 28, 2021, removal from the Robocall Mitigation Database effectively blocks a provider from participating in

---

[54] *Id.*

[55] Second Order at ¶ 24-27; Call Blocking Tools Available to Consumers: Second Report on Call Blocking CG Docket No. 17-59, A Report of the Consumer and Governmental Affairs Bureau, DA 21-772, at ¶ 14-16 (June 2021), *available at* https://www.fcc.gov/document/second-call-blocking-report-blocking-available-consumers; Department of Justice, Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, 2020 Report to Congress 13, *available at* https://www.justice.gov/opa/press-release/file/1331576/download [DOJ 2020 Report].

[56] DOJ 2020 Report at 14.

[57] Second Order at ¶ 78, 80-81.

[58] Second Order at ¶ 83.

the telephone system, because downstream providers are not permitted to accept the call traffic of the deficient provider.[59]

Additionally, in its recent Third Further Notice of Proposed Rulemaking (3NPR), the Commission required that "[v]oice service providers seeking the benefit of one of these extensions [including the two year extension for small voice providers] *must*…comply with requirements to respond fully and in a timely manner to all traceback requests from certain entities, effectively mitigate illegal traffic when notified by the Commission, and *adopt affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls."*[60]

Taken together, this indicates that the Commission has already provided more than adequate notice to providers that they will be removed from the Robocall Mitigation Database—and effectively blocked from introducing calls into the system—if they do any *one* of the following:

- Fail to comply with the provider's own stated mitigation program;[61]
- Fail to respond fully and in a timely manner to traceback requests;[62]
- Deliberately or through negligence serve as the originator for unlawful robocall campaigns;[63]
- Fail to effectively mitigate illegal traffic when notified by the Commission;[64]
- Fail to adopt affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls;[65] or

---

[59] 47 CFR § 64.6305(c). The prohibition went into effect on September 28, 2021. *See Wireline Competition Bureau Announces Opening of Robocall Mitigation Database and Provides Filing Instructions and Deadlines*, WC Docket No. 17-97, Public Notice, 36 FCC Rcd 7394 (WCB 2021).

[60] *In re* Call Authentication Trust Anchor, Third Further Notice of Proposed Rulemaking, WC Docket No. 17-97, at ¶ 4, *available at* https://ecfsapi.fcc.gov/file/05212146020718/FCC-21-62A1.pdf. [3NPR]. (Emphasis added.)

[61] Second Order at ¶ 78.

[62] 3NPR at ¶ 4.

[63] Second Order at ¶ 78.

[64] 3NPR at ¶ 4. While providers should be responsive to notification from the Commission, there are several points prior to such notification at which a provider should be removed from the Robocall Mitigation Database for non-compliance, for example being subject to a traceback request.

[65] 3NPR at ¶ 4.

- Fail to take reasonable measures to implement an effective call authentication framework.[66]

We recognize the Commission's continuing issuance of cease-and-desist letters for violative conduct. These letters have included requiring the provider to furnish a report on "concrete steps…to prevent a recurrence of these operations."[67] They have warned providers that further penalties may include authorizing U.S.-based voice service providers to block all call traffic, and eventually de-certification from the Robocall Mitigation Database[68] which would require, not merely authorize, other providers to block their traffic. In October 2021 the Commission issued the fourth tranche of cease-and-desist letters; and the Commission's official warnings to providers for not complying with their own program date back to October 2020, if not earlier.

Between public cease-and-desist letters and warnings from the Second Report and Order, non-compliant providers have received ample notice to comply with requirements such as traceback requests and their own self-certified mitigation programs. Additional specific warnings should no longer be necessary. The Commission should begin enforcing its rules regarding removing non-compliant providers from the Robocall Mitigation Database. As we noted in Section III(a) *infra*, this is an action the Commission can take against providers operating on non-IP networks as well as those operating on IP networks.

---

[66] Id.

[67] Federal Communications Commission, FCC Demands Three More Companies Immediately Stop Facilitating Illegal Robocall Campaigns (Oct. 21, 2021), *available at* https://docs.fcc.gov/public/attachments/DOC-376789A1.pdf.

[68] Letter to Duratel from Rosemary C. Harold (Oct. 21, 2021), *available at* https://docs.fcc.gov/public/attachments/DOC-376747A1.pdf.

V. Conclusion

We appreciate the opportunity to respond to the Commission's Notice and Request for Comments on the two-year extension for small voice service providers to comply with the STIR/SHAKEN protocol, and we are encouraged by the comments of the industry and of state regulators on this docket urging for more immediate action on this issue.[69] We urge the Commission to reduce the extension and to reject any further extension requests from providers who fail to satisfy both a compliance-based and a constructive notice-based evaluation methodology of their robocall mitigation efforts. We reiterate that a Commission determination about continuing extensions based on other factors, ones that fail to take in to account compliance and constructive notice, would frustrate incentives for certain providers[70] to comply with the rules and align their business practices with the goal of facilitating only legitimate calls.

Respectfully submitted, this the 12th day of November 2021, 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

[69] *See e.g.*, Comments of USTelecom, *supra* note 47; Comments of Transaction Network Services, Inc., WC Docket No. 17-97 (filed July 9, 2021), *available at* https://ecfsapi.fcc.gov/file/107091569107055/TNS%20July%202021%20Comments_3rd%20FNPRM_FINAL.pdf ; Comments of National Association of Attorneys General, WC Docket No. 17-97 (filed Aug. 9, 2021), *available at* https://ecfsapi.fcc.gov/file/10809277104737/FILED_Reply%20Comments_51%20AGs_Small%20VSPs%20and%20STIR-SHAKEN_WC17-97.pdf.

[70] For example, incentives for non-facilities-based providers would be undermined if the Commission were to grant or deny extensions based on whether a provider was facilities-based.