Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Numbering Policies for Modern Communications	)	WC Docket No. 13-97
	)	
Telephone Number Requirements for IP-Enabled Service Providers	)	WC Docket No. 07-243
	)	
Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources	)	WC Docket No. 20-67

COMMENTS ON THE FURTHER NOTICE OF PROPOSED RULEMAKING

by

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

Submitted October 14, 2021

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

Megan Iorio
Counsel
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

Carolyn Carter
Deputy Director
National Consumer Law Center
1001 Connecticut Ave, NW
Washington, DC 20036

Summary

We applaud the Commission's initiation of a regulatory process to consider the best ways to increase accountability for VoIP providers by limiting their direct access to numbers pursuant to Section 6 of the TRACED Act. That section requires the Commission to determine "how Commission policies regarding access to number resources . . . could be modified [to ensure] that providers of voice service given access to number resources take sufficient steps to know the identity of the customers of such providers . . . ."[1] The idea behind Section 6 is to put the onus on the VoIP providers to ensure that the parties to whom they are providing access to the American telephone system are complying with the rules. Given the ongoing invasion of robocalls to America's telephones, this effort—along with others initiated by the Commission—are clearly much needed.

The Commission's proposals in the Further Notice of Rulemaking and Proposed Rules are a good start. However, more specific rules, more clarity, and more mandates are also needed. On behalf of consumers, we urge the Commission to provide and implement the following:

1. More explicit guidance to providers on what **activities should be considered indicators** of an illegal robocall operation, including a non-exhaustive list of such indicators.
2. A list of **methods providers should be required to use** to maximize their opportunities **to spot these indicators** of an illegal robocall operation.
3. Specific **actions providers should be required** to take once the indicators are apparent.
4. A clear statement that a **provider's failure** to a) use either the Commission's proposed methods of spotting illegal robocall operations or a different but equally effective method, and b) shut down access to the callers conducting an illegal robocall operation, will lead to the **suspension and possible permanent expulsion of the provider** from the numbering system.
5. Greater transparency to consumers and to providers regarding sources of **potential robocall threats.**

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

These measures will help to fulfill the mandates of the TRACED Act in a way that supports providers and consumers alike.

We also ask that the Commission provide clarification that the Know Your Customer requirements will only apply to commercial callers, as Commission publications have not always explicitly noted that non-commercial callers would be excluded from these requirements.

Table of Contents

Comments

I. Introduction

The Federal Communications Commission (Commission) issued a request for comments in a Further Notice of Proposed Rulemaking and Proposed Rules[2] as required by the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act[3] relating to access to numbering resources, and other relevant practices to reduce illegal robocalls. The **Electronic Privacy Information Center (EPIC)**,[4] and the **National Consumer Law Center[5] (NCLC)** on behalf of its low-income clients, file these comments in response to the Commission's proposal to adopt rules setting forth the specifics for reducing access to telephone numbers by potential perpetrators of illegal robocalls.

The Commission's proposal to require VoIP providers applying for direct access to numbers to certify that the applicant will use numbering resources lawfully is a good start. However,

---

[2] *See* Federal Communications Commission, Numbering Policies for Modern Communications, Proposed Rules, WC Docket Nos. 13-97, 07-243, 20-67, IB Docket No. 16-155, 86 Fed. Reg. 51,081 (Sept. 14, 2021) [hereinafter Proposed Rules].

[3] TRACED Act, *supra* note 1.

[4] 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.

[5] 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*.

considerably more specifics are necessary, as mere certification will not effectively mitigate robocalls—there must be more explicit guidance and deterrence.

The overarching principles for the Commission's implementation of its TRACED Act responsibilities should include transparency, public access to information, and clear authority for state and private entities to enforce the requirements. All of these are necessary to ensure robust mobilization of the TRACED Act's requirements to combat the scourge of robocalls.

The Commission can achieve this by requiring providers to take sufficient steps to detect indicators of robocall activity and to respond adequately to detected threats. The Commission should provide a list of indicators to providers, articulate what the consequences of non-compliance will be, and facilitate information-sharing about potential threats amongst providers and consumers.

The TRACED Act mandates that the Commission determine appropriate requirements to impose on voice service providers to know the identity of their customers, in order to reduce access to numbers by potential TCPA violators, and also requires that the Commission prescribe corresponding regulations.[6] Congress also explicitly granted the Commission the authority to apply a forfeiture penalty for violators of these requirements, in addition to any other penalties provided for by law.[7]

The TRACED Act also requires the Commission to consider the best means of ensuring that a subscriber or provider has the ability to block calls from a dialer using an unauthenticated North American Numbering Plan (NANP) number.[8]

These comments are organized as follows:

- Section II provides an extensive but non-exhaustive list of what facts may be indicative of the occurrence of unlawful robocalls.

[6] 47 U.S.C. § 227b-1(a).

[7] 47 U.S.C. § 227b-1(b).

[8] TRACED Act. at § 7(b)(2).

- Section III suggests several methods that providers should be required to use—unless they implement equally effective methods—to ensure that they are verifying that those indicators are *not* present.
- Section IV includes suggestions for how a provider should be required to respond to indicators that dialers are making unlawful robocalls.
- Section V recommends efforts to increase threat transparency to consumers and providers.
- Section VI proposes measures the FCC should employ to encourage compliance from providers and deter the continuing scourge of illegal robocalls.
- Section VII contains an important request for clarification regarding the privacy implications of a Know Your Customer regime.

II. Establish Detailed Indicators of Illegal Robocall Activity

We support the Commission's proposal to require an applicant relying on a robocall mitigation program "to certify that it has described in the Database the detailed steps it is taking regarding number use that can reasonably be expected to reduce the origination and transmission of illegal robocalls."[9] However, certifications should also include commitments to monitor for indicators of illegal robocall activity, and in more explicit terms than generic statements such as "vets all of its customers by collecting a wide variety of data including contact information" or "[w]e use a third-party service that rejects calls that are deemed likely illegal robocalls."[10]

To that end, we suggest that the Commission articulate more explicit guidance to providers regarding what activity is likely to indicate that illegal robocalls are occurring, including a non-exhaustive list of such indicators. The following are examples of indicators the Commission should adopt, drawn from a diverse set of sources. We recognize that there are overlapping ideas in this list, and suggest that some redundancy to ensure coverage is preferable to inadvertent omission of

[9] Proposed Rules, *supra* note 2, at ¶ 4. The Commission also asked "Are there specific practices we should require applicants to address in their certifications?" Id. at ¶ 3.

[10] Legal Calls Only, Evaluating Robocall Mitigation Programs (Dialer Five Telco – Inadequate Plan), *available at* https://legalcallsonly.org/mitigation/ .

important indicators. Any one of these criteria should trigger the Know Your Customer compliance regimen for the providers.

Indicators of illegal robocall activity in caller behavior:

- High frequency of calls per minute.[11] Note that the high number of calls per minute is an important gauge of robocalls, but if the Commission establishes any specific number—as recommended in the original suggestion in the citation—robocallers can simply set their dialers to make one less than the target number of calls per minute and avoid tripping the compliance needle. To avoid this, the Commission should not set a specific number.
- Record of buying local numbers in bulk.[12]
- Average call duration less than three minutes.[13]
- Fewer than 80% of calls lasting longer than two minutes.[14]
- Consumer complaints, especially if the calls originate outside the US.[15]
- More calls per hour than could reasonably be expected to be manually dialed in human-to-human calling if (1) the provider has not vetted the caller and (2) the provider has received complaints about the caller that have not been resolved.[16]
- Call center origination, combined with short call duration.[17]
- Banks of direct inward dialers (DID)s to capture callbacks.[18]
- Refreshing number banks regularly by purchasing new blocks of numbers and discontinuing old blocks.[19]
- Sequential dialing patterns.[20]
- Significant volumes of calls to numbers in the FTC's Do Not Call registry.[21]

---

[11] *See* David Frankel, Legal Calls Only, *Structuring an Effective Robocall Mitigation Program* (Mar. 16, 2021), *available at* https://legalcallsonly.org/structuring-an-effective-robocall-mitigation-program/. Call frequency is distinct from but related to "high-volume" network traffic. *See* USTelecom, Whitepaper: How to Identify and Mitigate Illegal Robocalls 8 (Oct. 2019), *available at* https://www.ustelecom.org/wp-content/uploads/2019/11/USTelecom-Whitepaper-Combating-Illegal-Robocalls.pdf [hereinafter USTelecom Whitepaper].

[12] *See* Hiya, EBook, How to Stop Spoofing: Protect Your Customers From Spammers & Scammers, *available at* https://www.hiya.com/resources.

[13] *See* David Frankel, Legal Calls Only, *Myth-Busting Call Blocking* (Sept. 17, 2021), *available at* https://legalcallsonly.org/myth-busting-call-blocking/.

[14] *Id.*

[15] *See* David Frankel, Legal Calls Only, *My Suggestion for a Declaratory Ruling* (May 22, 2019), *available at* https://legalcallsonly.org/my-suggestion-for-a-declaratory-ruling/.

[16] *See id.*

[17] *See* David Frankel, *Legal Calls Only, Illegal Robocalling For Fun & Profit: The Why and How of Nefarious Mass Calling* (Sept. 25, 2019), *available at* https://legalcallsonly.org/wp-content/uploads/Hiya-HowTo-2019.pdf.

[18] *See id.*

[19] *See id.*

[20] *See* US Telecom Whitepaper, *supra* note 11, at 8.

[21] *See id.*

- Disparities between expected use (including call patterns) with actual usage.[22]
- Number of unique caller-ID values equals number of calls.[23]
- Provided false, inaccurate, or misleading information in response to a provider's screening process.[24]

Additionally, providers should be required to monitor the activities of upstream providers, whose calls they are transmitting, and should be required not to transfer calls from those providers.

Indicators of illegal robocall activity in originating or intermediary providers:

- Weak Robocall Mitigation Plans (RMPs) that also exhibit other suspicious factors. (A weak program does not adequately vet customer legitimacy, limit simultaneous calling, constrain use of Caller-ID values, monitor traffic, or cooperate with tracebacks).[25]
- Allows callers excessively high limits on maximum calls per minute.[26]
- Delegates SHAKEN signing to downstream providers that sign all calls as Partial B. (This was a trend discovered within the first three months following the SHAKEN attestation mandate).[27]
- Record of failing to confirm that each number originating on its network is either assigned directly to the customer or that it is being used by the customer with the explicit permission of the assignee.[28]
- 15% or more calls in a single day that pass through its network that last thirty seconds or less.[29]
- 50% or more calls in a single day that pass through its network that last sixty seconds or less.[30]

---

[22] *See* Frankel, *Structuring an Effective Robocall Mitigation Program*, *supra* note 11.

[23] *See* Frankel, *Myth-Busting Call Blocking*, *supra* note 13.

[24] Nessel *ex rel.* Michigan v. All Access Telecom Inc., No. 20-39—CP, Assurance of Voluntary Compliance, at 20 (Mich. Sept. 11, 2021), *available at* https://www.michigan.gov/documents/ag/Assurance_of_Voluntary_Compliance_-_All_Access_Telecom_FINAL_9-11-20_702047_7.pdf [hereinafter All Access].

[25] We do not necessarily endorse the scoring method described at https://legalcallsonly.org/introducing-the-zipdx-robocall-mitigation-database-explorer/ and at https://legalcallsonly.org/mitigation/, but merely offer it as an example of how RMPs might be evaluated.

[26] *See* Frankel, *Illegal Robocalling For Fun & Profit: The Why and How of Nefarious Mass Calling*, *supra* note 17.

[27] *See* TransNexus, Spam robocalls and SHAKEN attestation (July 26, 2021), *available at* https://transnexus.com/blog/2021/robocall-attestation-stats-july/.

[28] *See* Frankel, *Structuring an Effective Robocall Mitigation Program*, *supra* note 11.

[29] *In re* VC Dreams USA LLC d/b/a Strategic IT Partner, Assurance of Discontinuance, at 9 (Vt. Super. Ct. Apr. 19, 2021), *available at* https://ago.vermont.gov/wp-content/uploads/2021/04/Executed-AOD-SITP.pdf [hereinafter VC Dreams].

[30] *Id.*

- Originates or transmits calls from customers who have been subject to two or more traceback requests.[31]
- Has been determined by USTelecom to be a "Non-Cooperative Voice Service Provider."[32]
- Has been determined by the FCC to be a "bad-actor upstream voice service provider."[33]
- Provided functionality that allowed customers to mask their identities.[34]

A detailed, non-exhaustive list of robocall indicators would put providers on notice of the types of activity they must monitor and respond to—and allow the Commission to take action against those who do not.

III. Require Providers to Implement Methods to Detect and Investigate Possible Robocall Activity

Additionally, the Commission should mandate that providers actively monitor for the indicators of illegal robocall activity, and require that providers not facilitate those calls. To accomplish this, the Commission should articulate a set of best practices for providers to spot illegal robocall activity. The Commission's guidance should include a non-exhaustive list of methods that providers should use to monitor for indicators of illegal robocalls. Providers should be required to engage in both initial vetting of callers, as well as ongoing monitoring, as bad actors seem quite capable of presenting themselves to be the proverbial wolf in sheep's clothing.

Section 6(a) of the TRACED Act, codified as 47 U.S.C. § 227(b-1), provides that the Commission:

---

[31] All Access, *supra* note 24, at 16. In the cited document, the parties agreed to a standard of three or more traceback requests in a single year related to prerecorded messages where the customer terminated fewer than fifty million calls into a single network, or seven or more traceback requests where the customer terminated more than fifty million calls across any number of networks. We do not recommend including such qualifiers and instead propose a universal standard of two or more traceback requests.

[32] All Access, *supra* note 24, at 12; VC Dreams, *supra* note 29, at 4.

[33] All Access, *supra* note 24, at 13; VC Dreams, *supra* note 29, at 4. The FCC considers upstream providers who fail to effectively mitigate illegal traffic after being notified of such traffic to be bad actors. Fact Sheet, Federal Commc'ns Comm'n, *Targeting Gateway Providers to Combat Illegal Robocalls*, CG Docket No. 17-59, WC Docket No. 17-97, at ¶ 20, *available at* https://docs.fcc.gov/public/attachments/DOC-375612A1.pdf.

[34] Mey v. All Access Telecom, Inc., Civil Action No. 5:19-cv-00237-JPB, Order Denying Motions to Dismiss, at 9 (N.D. W. Va. Filed Apr. 23, 2021), *available at* https://www.dwt.com/-/media/files/blogs/broadband-advisor/2021/05/mey-v-all-access-telecom-order-denying-carrier-mtd.pdf.

> (1) … shall commence a proceeding to determine how Commission policies regarding access to number resources, … could be modified, including by establishing requirements that providers of voice service given access to number resources take sufficient steps to know the identity of the customers of such providers, to help reduce access to numbers by potential perpetrators of violations of section 227(b) of the Communications Act of 1934 (47 U.S.C. 227(b)).[35]

And that

> (2)…If the Commission determines under paragraph (1) that modifying the policies described in that paragraph could help achieve the goal described in that paragraph, the Commission shall prescribe regulations to implement those policy modifications. [36]

We suggest that the Commission not merely implement a Know Your Customer regime for **commercial customers**, whereby service providers are responsible for verifying the identity of their customers, but also **require that providers take sufficient steps to continue to monitor those commercial customers for indicators of illegal robocalling**. This is consistent with Section 7 of the TRACED Act, which provides that the Commission:

> (a) … shall initiate a rulemaking to help protect a subscriber from receiving unwanted calls or text messages from a caller using an unauthenticated number.
> (b) Considerations.--In promulgating rules under subsection (a), the Commission shall consider--
> …
> (2) the best means of ensuring that a subscriber or provider has the ability to block calls from a caller using an unauthenticated North American Numbering Plan number;
> (3) the impact on the privacy of a subscriber from unauthenticated calls;
> (4) the effectiveness in verifying the accuracy of caller identification information; and
> (5) the availability and cost of providing protection from the unwanted calls or text messages described in subsection (a).[37]

A coalition of State Attorneys General and telecom providers also recommend that providers should be explicitly required to monitor traffic on their networks and investigate suspicious patterns. One of their requirements entails analyzing high-volume voice traffic,[38] and the

---

[35] 47 U.S.C. § 227b-1(a)(1) (emphasis added).

[36] 47 U.S.C. § 227b-1(a)(2) (emphasis added).

[37] TRACED Act, *supra* note 1, at § 7.

[38] Anti-Robocall Principles for Voice Service Providers, Principle #3 (2019), *available at* https://oag.ca.gov/system/files/attachments/press-docs/State%20AGs%20Providers%20AntiRobocall%20Principles-With%20Signatories.pdf [hereinafter Anti-Robocall Principles].

other requires verifying the Caller ID sent to the receiving party.[39] We agree with these suggestions and recommend that the Commission adopt them.

USTelecom urged recently that voice service providers be required to monitor all high-volume network traffic.[40] It charged originating providers with the responsibility to take action where the evidence suggested illegal robocalling has occurred, and similarly emphasized that downstream providers should be considered responsible for taking action when the originating provider has failed to.[41] USTelecom also said that downstream providers should be required to notify offending originating providers of "terms-of-service and/or acceptable-use-policy violations."[42] We agree with these suggestions and recommend that the Commission adopt them. These responsibilities are meaningless however if there are not consequences for failing to fulfill them, as we discuss in Section VI, *infra*.

One effective illustration of how a VoIP provider might be required to engage in ongoing monitoring of its customer-callers was made by a provider of services to callers. In the provider's example, the requirements of an ongoing monitoring regime should include call-by-call confirmation that the caller-ID used is on the pre-validated list, that the calling rate and other usage characteristics are consistent with the type of calling the customer represented that it would be making, and that calls are not being reported as illegal.[43]

Based on the indicators listed in Section II, *supra*, providers should also be required to monitor call characteristics, caller characteristics, and general compliance characteristics of their

---

[39] *Id.*, Principle #4.

[40] *See* US Telecom Whitepaper, *supra* note 11, at 8.

[41] *See id.*

[42] *See id.*

[43] Frankel, *Structuring an Effective Robocall Mitigation Program, supra* note 11.

callers and the upstream providers. If any of the indicators are spotted in monitoring these characteristics, providers should be required to take the steps outlined in Section IV, *infra*.

The characteristics providers should be required to monitor and measure are the following:

Call characteristics:

- The frequency of calls to determine if mass dialers are used.
- The duration of calls to determine if calls are disconnected quickly.
- The ratio of calls to caller-ID values to determine if the callers are falsifying caller-IDs.

Caller characteristics:

- Whether calls are originated outside the United States.
- Whether calls are made from call centers which would be indicative of robocalls.
- The use of direct inward dialing (DID) to capture callbacks, which would be indicative of callers that do not have consent to make the automated calls.
- The purchase of local numbers in bulk.
- The rate at which the number bank is refreshed.

Compliance characteristics:

- The volume of consumer complaints.
- The volume of provider complaints.
- The strength or weakness of a provider's Robocall Mitigation Plan (RMP).
- Whether the provider delegates SHAKEN signing.

The Commission should provide a minimum set of requirements, including these factors. Additionally, beyond its own requirements, the Commission should offer some measure of guidance regarding the stringency and reliability of other methods providers may choose from to demonstrate their commitment to developing an awareness-towards-action regarding how illegal robocalls are being facilitated on their networks. The agreement signed between the state AGs and twelve major voice providers, along with the Whitepaper by USTelecom, both include recommendations for ongoing monitoring of this type. We propose that the FCC make more explicit what that monitoring should look like. USTelecom's suggestion that downstream providers notify offending originating providers appears to be a particularly helpful means of ensuring that offending originating providers

are made aware of the violations that are occurring as a result of their behavior. We agree with USTelcom's suggestion and urge the Commission to adopt it. However, this will be effective only if downstream providers are themselves taking sufficient steps to monitor their traffic and complaints regarding that traffic.

IV. Establish the Threshold for an Adequate Provider Response upon Detecting Indicators

When illegal robocall activity is detected, providers should be required to block access to the telephone network for the callers and upstream providers responsible for originating or facilitating the calls. The Commission must make clear to providers that they are responsible for acting upon information they obtain about robocall threats moving through their networks. The Commission should also detail what the minimum threshold for compliance will be. We propose, as a minimally adequate measure, that providers immediately terminate customer and/or provider access to the network and allow the blocked customer or provider to appeal the termination decision.

Providers are in the best position to protect consumers from the callers who are making unlawful robocalls. Congress recognized this, which is why Section 7(b)(2) of the TRACED Act demands that the Commission consider:

> (2) the best means of ensuring that a subscriber or provider has the ability to block calls from a caller using an unauthenticated North American Numbering Plan number;

Indeed, Section 7 of the TRACED Act provides a key method for providers to act upon the information they have gathered: simply by blocking the calls made by the offending caller, or the calls originated or transmitted by the offending provider.

The anti-robocall principles adopted by the state AGs and the dozen telecom providers urged that providers who suspect that illegal robocalling or spoofing is occurring through their network verify that the originating commercial customer owns or is authorized to use the Caller ID number, determine whether the Caller ID sent matches the customer's name, terminate the party's

ability to originate, route, or terminate calls, and notify law enforcement authorities.[44] These are excellent requirements that the Commission should explicitly impose on providers.

USTelecom has also urged that originating providers who learn their platform is being used as a conduit for illegal robocalls should impose network level constraints "which can include throttling the rate at which the customer can initiate calls, restricting the number of concurrent calls, and limiting the caller-ID value(s) available for the customer's use." It further suggests discontinuance of service, if violations are ongoing.[45] We propose that these originating providers be *required* to impose these network level constraints.

Downstream providers should be obligated to refuse traffic from originating providers that violate these requirements. The Commission should require downstream or intermediate providers be alert to the indicators of illegal activities and refuse to process calls from violators. USTelecom has endorsed this kind of tough approach.[46]

While some advocate that the provider should warn the offending customer before terminating the customer, given the common recognition of the huge problem of illegal robocalls, and the likely efforts of many callers to try to evade these mitigation efforts, we recommend that one violation of the rules should lead to automatic termination of services by the provider. The customer might then be permitted the opportunity to show why that termination was in error. The burden should be on robocallers to show that they are *not* violating the law.

Providers who do not include or do not enforce such terms in contracts with their customers should be subject to greater scrutiny by the Commission.[47] One service provider for

---

[44] Anti-Robocall Principles, *supra* note 38, Principle #4.

[45] *See* US Telecom Whitepaper, supra note 11, at 8.

[46] *See* US Telecom Whitepaper, supra note 11, at 9.

[47] Or specifically by the Wireline Competition Bureau, as proposed in the Proposed Rules, *supra* note 2, at ¶ 26.

callers has affirmed that "[p]roviders are expected to require their customers to abide by those provisions and to take appropriate action if they do not….[O]nce a provider becomes aware that they are an enabler for illegal traffic, they are fully empowered to do something about it and don't need any further authority or permission from the FCC." [48]

V. Make the Threats Submitted via the Complaint Portals—Especially via the Provider Complaint Portal—More Transparent to Providers and to Consumers

The Commission should also compile a consolidated list of providers with a high likelihood of engaging in or permitting robocalling and make this list conveniently accessible to the public. This list could include entities it has determined to be "bad-actor upstream voice service providers"[49] and/or have been deemed "non-cooperative voice service providers" by USTelecom. We are encouraged by the Commission's efforts to create a portal whereby providers can report suspicious activity occurring on their networks,[50] as this may reduce the likelihood of a bad actor simply rotating providers when it gets caught and its access is terminated by one provider.

However, unlike the Information Sharing and Analysis Organizations that collaborate in addressing threats to our nation's cybersecurity,[51] the process that the Commission has set up is not necessarily transparent in a way that informs providers about suspicious activity prior to the outcome of an FCC investigation. Both providers and injured consumers should be empowered to take action on their own, be that a commercial or a legal action, without needing to wait upon a determination from the Commission. USTelecom has suggested that private entities coordinate with

---

[48] David Frankel, Legal Calls Only, *FCC Enforcement Affirms Providers' Ability and Expectation to Mitigate Illegal Calls & Share Info* (Mar. 25, 2019), *available at* https://legalcallsonly.org/fcc-enforcement-affirms-providers-ability-and-expectation-to-mitigate-illegal-calls-share-info/ .

[49] The FCC considers providers who fail to effectively mitigate illegal traffic after being notified of such traffic to be bad actors. *See* FCC, *Targeting Gateway Providers to Combat Illegal Robocalls*, *supra* note 33, at ¶ 20.

[50] *See* Federal Communications Commission, Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), Final Rule, 86 Fed. Reg. 52,840 (Sept. 23, 2021).

[51] *See* United States Cybersecurity & Infrastructure Security Agency, Information Sharing and Analysis Organizations (ISAOS), *available at* https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos.

the registered traceback consortium.[52] We agree with this suggestion generally, as this is closer to current best practices in mitigating cybersecurity threats and we encourage the FCC to adopt a similar approach in empowering all stakeholders to address robocall threats. Such a protocol would only serve its intended purpose if providers are required to contribute information necessary to keep the landscape of robocall threats up to date. This relates back to expectations the Commission should set with providers, in terms of how a provider is expected to respond when it becomes aware of the indicators that illegal robocalling is occurring on its networks, as addressed in Section IV, *supra*.

VI. Articulate Commission Responses to Noncompliant Providers

We request that the Commission also clarify what actions it will take if providers fail to respond adequately to indicators of illegal robocalls. Providing a list of robocall indicators to monitor, methods by which they should be monitored, and responses that the Commission would expect a provider to take will be sufficient for those providers who make mitigating the robocall issue a top priority (as it is the Commission's[53]). However, some providers will only be motivated to comply if the Commission adopts strict penalties for noncompliance, such as forfeiture.

Section 6(b) of the TRACED Act, codified as 47 U.S.C. § 227b-1(b) allows the Commission to impose a forfeiture penalty on providers who violate the Commission's regulation to exclude illegal robocallers from numbering resources. A service provider who has disregarded the ample guidance of the Commission should be considered to have willfully neglected its responsibilities to mitigate robocalls, warranting a forfeiture remedy.

---

[52] *See* USTelecom Whitepaper, supra note 10, at 7, 8; *also see* Federal Communications Commission, Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), Final Rule, 86 Fed. Reg. 52,840, at ¶ 12 (Sept. 23, 2021).

[53] "Unwanted calls—including illegal and spoofed robocalls—are the FCC's top consumer complaint and our top consumer protection priority." *See* Federal Communications Commission, Stop Unwanted Robocalls and Texts, *available at* https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts.

We encourage the Commission to clarify the range of potential actions it will take to ensure prompt compliance and deter continuing noncompliance among providers who fail to take sufficient steps to mitigate robocalls. Such clarification should include, for example, the use of forfeiture as a remedy, and make explicit which entities would be liable. We also ask the Commission to implement policies that would facilitate the effective steps already being taken by state Attorneys General and individual consumers.

The Federal Trade Commission last year brought an action seeking injunctive relief and disgorgement from a provider who contacted individuals on the National Do Not Call Registry, transmitted calls that delivered prerecorded messages, and transmitted inaccurate caller ID information.[54] The FCC should similarly seek penalties not less than the collective profit made by each provider and customer who permitted the illegal calls to be transmitted over their network, and let those parties seek contribution from one another in sorting out the proportion of responsibility for the violations.

State Attorneys General have already taken action to protect consumers against irresponsible providers. The FCC should seek similar types of relief, and/or use its authority to facilitate state AGs and consumers being able to do so. Consent orders obtained by state AGs have included conducting reasonable screening and call monitoring of customers, and requiring the provider's customers to sign agreements that hold the customers to notification and verification/traceback standards, with a monetary penalty for each violation of these terms.[55] They have also included: requiring customers to provide documentation of their policies for ensuring calls are not placed to

[54] Federal Trade Commission v. Alcazar Networks Inc., Case No. 6:20-cv-2200, Complaint for Permanent Injunction and Other Equitable Relief (filed Dec. 3, 2020), *available at* https://www.ftc.gov/system/files/documents/cases/1_-_complaint_0.pdf.

[55] *See* VC Dreams, *supra* note 29.

persons registered on the Do Not Call Registry[56] or using prerecorded messages without evidence of express written consent;[57] taking reasonable efforts to verify that the affirmations the customer has made to them are accurate;[58] and providing reports upon request of the provider's compliance with the consent order.[59]

Additionally, the FCC should ensure that individual consumers can seek relief for themselves. Individuals have successfully obtained judgments against providers for facilitating illegal robocall activity, and these actions should continue to be encouraged. For example, one federal district court recently determined that the TCPA could provide a remedy to a consumer harmed by an intermediate provider who failed to take sufficient action to prevent robocalls from being transmitted over its network.[60] However, we stress that the burden should never be on the consumer to mitigate illegal robocalls, but rather upon the providers who facilitate and profit from the offending calls.

VII. Clarify the Scope of Know Your Customer Requirements, to Avoid Potential Consumer Privacy Concerns

In the process of seeking greater responsibility and accountability for VoIP providers, we also want to ensure that the methods the Commission advances do not inadvertently result in a loss of privacy for individual consumers due to additional data collection. As such, we ask the Commission to clarify that the scope of Know Your Customer verification and vetting is limited to commercial customers only.[61]

---

[56] *See* All Access, *supra* note 24, at 9.

[57] *See id.*

[58] *See id.* at 13-14.

[59] *See id.* at 21.

[60] May v. All Access Telecom, Inc., *supra* note 34.

[61] The Commission's proposal asks, "Should we require applicants to certify that they 'know their customer' through customer identity verification, as the Commission raised previously?" Proposed Rules, *supra* note 2, at ¶ 3.

The citation that follows the Commission's proposal regarding customer identity verification directs readers to previous publications DA 20-1526 Wireline Competition Bureau Issues Caller ID Authentication Best Practices (released Dec. 22, 2020) [hereafter Caller ID Best Practices], and to FCC 20-42 Report and Order and Further Notice of Proposed Rulemaking (released Mar. 31, 2020) [hereafter FNPR].

The first, more recent, document, Caller ID Best Practices, specifies that vetting would apply to retail and wholesale subscribers, "with the general goal of confirming the identity of their commercial customers."[62] It cites to sections 3.1.3-3.1.4 of the Best Practices for the Implementation of Call Authentication Frameworks by the NANC Call Authentication Trust Anchor Working Group [hereafter Council Report], which outlines best practices for vetting retail and wholesale Customers. Immediately above this cited portion of the Council Report however, the authors distinguish between End-Users and Customers[63] then go on to say that providers should vet subscriber identity in either case, suggesting the possibility of "collect[ing] distinct sets of information to vet the identity of residential End-Users, commercial End-Users, wholesale Customers, and other Resellers."[64] There has been no evidence to suggest that residential End-Users are a major source of robocalls, and so data collection about them is unlikely to mitigate robocalls and is likely to result in additional and unnecessary surveillance of consumers.

---

[62] Public Notice, Federal Commc'ns Comm'n, Wireline Competition Bureau Issues Caller ID Authentication Best Practices, WC Docket Nos. 17-97, 20-234, at ¶ 12 (Rel. Dec. 22, 2020) (citing Council Report, *infra* note 63).

[63] Call Authentication Trust Anchor Working Group, North American Numbering Council, Best Practices for the Implementation of Call Authentication Frameworks § 3.1.1 (2020), *available at* https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf.

[64] *Id.* at § 3.1.2.

Similarly, the FNPR does not appear to limit the scope of its Know Your Customer inquiry to commercial customers. Indeed, it asks whether rules should be different for different industry segments.[65]

Principle #5 of the Anti-Robocall Principles for Voice Service Providers, signed by fifty-one State Attorneys General and twelve voice service providers, limits identity confirmation to commercial customers.[66] Similarly, in its Whitepaper "How to Identify and Mitigate Illegal Robocalls," USTelecom stated that "**Know Your Customer:** Voice service providers should confirm the identity of new commercial customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of customer's business."[67]

We ask the Commission to clarify that its proposed Know Your Customer certification requirement would apply only to commercial customers, and not to all customers. All of our recommendations in support of customer verification above operate from the assumption that the scope of Know Your Customer vetting would be limited to commercial customers only.

VIII. Conclusion

The overarching principles for the Commission's implementation of its TRACED Act responsibilities should include transparency, public access to information, and clear authority for state and private entities to enforce the requirements. All of these are needed to ensure robust mobilization in support of the TRACED Act's requirements to combat the scourge of robocalls.

---

[65] *In re* Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources, Report and Order and Further Notice of Proposed Rulemaking, WC Docket Nos. 17-97, 20-67, at ¶ 130, *available at* https://docs.fcc.gov/public/attachments/FCC-20-42A1.pdf.

[66] Anti-Robocall Principles, *supra* note 38, Principle #5.

[67] *See* US Telecom Whitepaper, *supra* note 11, at 8 (emphasis added for "commercial").

Where there is more than a scintilla of evidence that a provider has facilitated illegal robocalling, both upstream and downstream providers should be required to investigate. Where the investigation produces evidence of illegal activity, providers should respond with prompt suspension in the absence of immediate remediation. Noncompliance should be deterred both by financial sanctions (*e.g.* disgorgement if possible and/or forfeiture) and public disclosures regarding the consumer injury the offending providers have perpetrated. Moreover, even where a determination has not yet been made, consumers and providers should be informed about known risks associated with possible sources of robocalls.

We appreciate the Commission's interest in resolving this persistent issue facing America's consumers and support its promulgation of rules requiring that providers implement a Know Your Customer regime for their commercial customers. However, as we describe above, the Commission should provide more explicit guidance to providers regarding their responsibilities, should require prominent public disclosures regarding noncompliance, and should impose financial penalties sufficient to deter ongoing violations while also facilitating effective enforcement mechanisms enacted by state and private entities.

Respectfully submitted, this the 14th day of October 2021, by:

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

Megan Iorio
Counsel
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

Carolyn Carter
Deputy Director
National Consumer Law Center
1001 Connecticut Ave, NW
Washington, DC 20036