

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

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

**COMMENTS ON THE FIFTH FURTHER NOTICE OF PROPOSED RULEMAKING
(CG Dkt. No. 17-59) AND FOURTH FURTHER NOTICE OF PROPOSED
RULEMAKING (WC Dkt. No. 17-97)**

by

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

Submitted January 10, 2022

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

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

Summary

The **Electronic Privacy Information Privacy Center**, and the **National Consumer Law Center**, on behalf of its low-income clients, propose a series of steps that the Federal Communications Commission should take to limit the damage that gateway providers cause by transmitting illegal robocall and scam calls to American telephones. To incentivize full cooperation in these efforts by all providers in the call path, the Commission should make it clear that providers will be considered liable for consumer losses resulting from scam calls and illegal robocalls transmitted through their network that they knew or should have known were illegal. To provide providers with the necessary information to manage their call flow, and limit or eradicate their risk from these calls, the Commission should require public disclosure of substantiated traceback information. Providers can use that information to identify which providers sending calls to them have been the subject of repeated tracebacks, as repeated tracebacks are indications that traffic from these providers is likely to be problematic. The Commission should also declare that when providers continue to transmit illegal calls after notice from any source that the traffic is illegal, the providers will be automatically delisted from the Robocall Mitigation Database. Finally, the Commission should treat ongoing provider non-compliance as complicity with bad actor callers, bar them from participating in the telephone network, and unequivocally place the burden on the providers to avoid facilitating illegal calls.

Table of Contents

Summary	ii
I. Introduction	1
II. All Service Providers Should Be Responsible for Mitigating Illegal Robocalls and Scam Calls	4
III. The Commission Should Require Publication of Traceback Information to Better Equip Providers and Protect Consumers	8
IV. Effective Delisting from the Robocall Mitigation Database Should Automatically Follow Repeated Tracebacks Against Providers, Failure to Respond to Tracebacks, and Other Indicia of Non-Compliance	12
V. The Commission Should Treat Ongoing Provider Non-Compliance as Complicity with Bad Actor Callers.	15
VI. Conclusion	16

Comments

I. Introduction

The **Electronic Privacy Information Center (EPIC)**,¹ and the **National Consumer Law Center**² (**NCLC**) on behalf of its low-income clients, file these comments in response to the Notice of Proposed Further Rulemaking³ issued by the Federal Communications Commission (Commission or FCC), requesting comments on how to prevent foreign-originated illegal robocalls from entering the American telephone network through gateway providers. We encourage the Commission to provide incentives and clear mechanisms for all voice service providers to stop transmitting scam calls and illegal robocalls.

¹ **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.

² **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.

³ *See In re Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, CG Docket No. 17-59 and WC Docket No. 17-97 (Oct. 1, 2021), available at <https://docs.fcc.gov/public/attachments/FCC-21-105A1.pdf> [hereinafter Request for Comment].

As the Commission notes,⁴ fraudulent robocalls continue to bombard our telephone lines. To reduce these invasive and dangerous calls, it is essential that all providers in the call path have more skin in the game. As noted by others in this docket,⁵ and stated by Commissioner Starks: “illegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it.”⁶ Only when the providers *lose* more money by transmitting the illegal calls than they *make* by transmitting them, will providers have the incentive to stop transmitting these calls.

In the Federal Communication Commission’s 2021 Report to Congress, nine voice service providers were listed as refusing participate in three or more tracebacks in 2021, after they had also been listed for this same repeated refusal to cooperate in 2020. This continued refusal to comply with the Commission robocall mitigation methodologies should not be tolerated. Yet these providers are still permitted to transmit illegal calls into the American telephone system. These defiant providers are only a fraction of the *known* offending providers. Until the Commission requires public disclosure of substantiated tracebacks, downstream providers, as well as consumers who have been victims of the illegal calls facilitated by these providers, will never know the identity of the bad actors that continue to assault the American telephone network with impunity. Instead, we learn of them one at a time as individual cases are built and filed in the courts.⁷

⁴ See Request for Comment, *supra* note 3, at ¶¶ 4-6.

⁵ See Comments of Twilio Inc., CG Docket No. 17-59 and WC Docket No. 17-97, at 2 (filed Dec. 10, 2021), available at <https://ecfsapi.fcc.gov/file/12100788523948/Twilio%20Comments%20on%20Gateway%20Provider%20FNPRM%20vF121021.pdf>; Comments of iBasis, Inc., CG Docket No. 17-59 and WC Docket No. 17-97, at 9 (filed Dec. 10, 2021), available at <https://ecfsapi.fcc.gov/file/1211300118055/Gateway%20Comments.PDF>.

⁶ *In re* Call Authentication Trust Anchor, WC Docket No. 17-97 (Sept. 30, 2021) (Statement of Comm’r Geoffrey Starks), available at <https://docs.fcc.gov/public/attachments/FCC-21-105A3.pdf><https://docs.fcc.gov/public/attachments/FCC-21-105A3.pdf>.

⁷ See, e.g., Plaintiff’s Complaint for Civil Penalties, Permanent Injunction, Other Equitable Relief, and Demand for Jury Trial, *Indiana v. Startel Commc’n L.L.C.*, No. 3:21-cv-00150-RLY-MPB, 2021 WL 4803899 (S.D. Ind. Oct. 14, 2021).

A single bad actor caller can defraud thousands of Americans of millions of dollars in a month. Congress charged the FCC with stopping illegal robocalls in 2019. We urge the Commission to make 2022 the year that enforcement of anti-robocall methodologies becomes fully effective.

Providers must have a meaningful stake in protecting consumers' interests. To do that they should have the incentive to adapt to the evolving tactics of bad actor callers. We recommend that the Commission hold providers liable for all consumer losses resulting from illegal robocalls and scam calls. This is the surest way to have the highest number of qualified "cops on the beat" protecting consumers from harmful phone traffic. If not, some providers will invest in combatting robocalls and achieving compliance at their own expense, while others will continue to profit from facilitating problematic calls in flagrant non-compliance.

One of the most important steps that the Commission can take to give providers the ability and the incentive to protect consumers from illegal calls is to make traceback records public. Knowing which originating, gateway, and first intermediate providers have been the subject of traceback requests will enable providers to avoid accepting their calls. At the same time, the publication of the traceback data will also incentivize the downstream providers receiving the illegal calls to police the transmittal of these calls. The publication of the traceback records will mean that the Commission, state attorneys general, and private litigants will all be able to identify those providers who facilitate the entry of these calls into the U.S. telecommunications system, as well as those who chose to ignore the red flags indicating that the calls were illegal. Providers will know that they could face potential liability if they turn a blind eye to the evidence that the calls they transmit are illegal. The information discovered in tracebacks about providers who repeatedly initiate and transmit illegal calls belongs to the American public. The Commission should provide that information to the public.

The Commission should also immediately require downstream providers to block calls from upstream providers who do not respond to traceback requests fully or in a thorough manner, or are otherwise non-compliant, effectively delisting them from the Robocall Mitigation Database. Finally, the Commission should treat providers demonstrating continued non-compliance as acting in complicity with bad actor callers.

II. All Service Providers Should Be Responsible for Mitigating Illegal Robocalls and Scam Calls.

Gateway providers are the entry point into the American telephone network for foreign callers and as such are in a unique position to arrest the flow of harmful scam calls and illegal robocalls. Given the continuing high numbers of illegal calls that originate outside of the United States, it is clear that the gateway providers for this traffic find it too profitable to stop. This traffic will continue to be placed into the American telephone network until it is more expensive to do so than to not do so.

One way to drive up the expense for facilitating the entry of these illegal calls into the U.S. telecommunications system is for the Commission to articulate that the providers responsible for transmitting the illegal traffic can be held liable for doing so. This responsibility should be applied to all providers in the call path who have the ability to identify characteristics of calls that are likely problematic, specifically including those calls originated by or transmitted through providers known to have been the subject of multiple tracebacks.

Clearly placing the cost of noncompliance on the providers downstream from the gateway providers and initial intermediary providers immediately downstream from the gateway providers will incentivize both those providers, and the providers downstream from them, to develop ways to ensure that they are not transmitting the illegal calls. The Commission should task all providers with

paying attention to the traffic that passes through their network, rather than wait for the FCC to present them with information that they have transmitted illegal calls that have harmed consumers.

Compliance with the requirement to pay attention to their own traffic is best enforced by assessing monetary damages against providers who repeatedly allow the illegal traffic to flow. As the Commission has found in similar contexts,⁸ taking an action while knowing that harm is substantially certain to occur amounts to intent to do harm. Continuing to transmit illegal traffic after receiving one or more traceback requests for that bad actor meets this standard.

To this end, we strongly support the Commission’s proposal to impose a general duty on gateway providers to mitigate illegal robocalls.⁹ Moreover, along with several other commenters, we encourage the Commission to impose a similar duty to mitigate on all providers.¹⁰ The Commission

⁸ See, e.g., Request for Comment, *supra* note 3, at ¶ 4 n.14 (citing to Rules and Regulations Implementing the Truth in Caller ID Act of 2009, WC Docket No. 11-39, Report and Order, 26 FCC Rcd 9114, 9122, ¶ 22 (2011)); see also Affordable Enterprises of Arizona, LLC, Notice of Apparent Liability for Forfeiture, 33 FCC Rcd 9233, 9242-43, ¶ 26 n.70 (2018) (citing Restatement (Second) of Torts § 8A, comment b, at 15).

⁹ See Request for Comment, *supra* note 3, at ¶¶ 51, 78, 91-92.

¹⁰ *Id.* See also Comments of USTelecom – The Broadband Association, CG Docket No. 17-59 and WC Docket No. 17-97, at 2 (filed Dec. 10, 2021), available at <https://ecfsapi.fcc.gov/file/12101593911611/USTelecom%20-%20Comments%20on%20Gateway%20Providers%20FNPRM%20-%20Final.pdf> [hereinafter USTelecom Comments] (“In particular, the Commission should streamline and enhance its approach to the RMD by closing the intermediate provider loophole and requiring that all providers, regardless of their role in the call path and whether or not they have implemented STIR/SHAKEN, implement a robocall mitigation program. In particular, as part of their robocall mitigation programs, intermediate providers should be expected to accept traffic only from other providers in the RMD. Enhancing the Commission’s existing RMD approach – *combined with active auditing of deficient database entries and aggressive and rapid enforcement* – will help to foment trusted full call paths without causing unnecessary confusion and leaving opportunities for gamesmanship as a focus just on gateway providers would.”) (emphasis added). ZipDX notes in its comments: “ALL providers in the path must play a role and be held accountable. Most efficient is stopping calls at the source, but to the extent that is not effective, enforcement efforts must move rapidly downstream, supported by appropriate underlying rules.” Comments of ZipDX L.L.C., CG Docket No. 17-59 and WC Docket No. 17-97, at 10-11 (filed Dec. 7, 2021), available at <https://ecfsapi.fcc.gov/file/12080110629539/ZipDX-17-97-GatewayComments.pdf> [hereinafter ZipDX Comments]. ZipDX also states that “[a]ll providers must be responsible. Enforcement efforts should be prioritized based on call volume and recidivism, with commensurate penalties.” *Id.* at 14.

has relied on its authority under the TRACED Act when adopting mitigation duties.¹¹ Also, the TRACED Act specifically authorizes “affirmative, effective measures” to be used to mitigate illegal calls, including in Sections 201(b), 202(a), and 215(e), as well as the Truth in Caller ID Act.¹²

The Commission is right to offer suggestions on how this mitigation might be accomplished. But we caution that rather than prescribe specific requirements to be included in a provider’s mitigation efforts, providers should simply have the strong financial incentive to figure out how best to adapt to bad actors’ changing tactics. That requires allowing providers flexibility in their methods. If providers are accountable for the *effectiveness* of their efforts, regardless of whether they employed one or five of the recommended steps, the marketplace will reward those providers who are most effective in mitigating the illegal calls.¹³ This is analogous to the protections credit card companies are required to provide to their consumers under the Fair Credit Billing Act.¹⁴ That Act does not tell institutions how to prevent frauds and other losses, but simply imposes on the banks, rather than consumers, the cost of losses from fraud, and even error, thereby incentivizing institutions to constantly improve their fraud detection and prevention tools.

¹¹ See Request for Comment, *supra* note 3, at ¶ 115 (“The Commission also relied on the TRACED Act in adopting mitigation duties for voice service providers and we propose to conclude that it authorizes us to require voice service providers to submit additional information to the Robocall Mitigation Database.”).

¹² See Request for Comment, *supra* note 3, at ¶ 116 (“In the Fourth Call Blocking Order, the Commission required voice service providers ‘to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls,’ which includes a duty to ‘know’ their customers. Additionally, the Commission required voice service providers, including intermediate providers, to ‘take steps to effectively mitigate illegal traffic when notified by the Commission,’ which may require blocking when applied to gateway providers. The Commission also adopted traceback obligations. The Commission concluded that it had the authority to adopt these requirements pursuant to sections 201(b), 202(a), and 251(e) of the Act, as well as the Truth in Caller ID Act and its ancillary authority.”).

¹³ The Commission seems to suggest something like this in its proposal to require gateway providers to adopt “affirmative, effective measures to prevent current, new, and renewing customers from using their network to transit illegal calls.” Request for Comment, *supra* note 3, at ¶ 92. Such an approach would also address the Commission’s concerns regarding under-blocking. *Id.* at ¶ 68.

¹⁴ The Truth in Lending Act precludes a credit card issuer from imposing liability on a customer (business or consumer) for unauthorized use of a credit card, except in narrowly defined circumstances. 15 U.S.C. § 1643.

We support the Commission’s proposal to require that immediately downstream intermediate providers block the call traffic of their respective gateway providers if the gateway provider fails to fulfill its duties to protect the American telephone network.¹⁵ Punishing downstream providers for processing the bad traffic from gateway providers is the most efficient method of stopping that bad traffic.

To accomplish these important changes, providers should not be permitted to wait to take action to mitigate robocalls until after receiving notification from the Commission if they possess information by which they could determine on their own that they are trafficking in illegal robocalls. As others have aptly noted in their comments: “while gateway providers’ current obligations to respond to traceback requests and to respond to Commission notifications of unlawful traffic are significant and beneficial, they are largely *reactive* in nature, and cannot take the place of *proactive* duties to mitigate harmful traffic directed towards the United States from abroad.”¹⁶ “By the time they [providers] hear from the FCC, their own monitoring tools, if they have any, have failed, and they have probably already been the subject of multiple traceback requests.”¹⁷

As the Commission is aware, there is also an urgent need for the Commission to impose a similar duty to mitigate live scam calls, which are likely made through an autodialer, thus qualifying as a robocall under the Commission’s rules even if those calls do not initially appear to be facilitated by a prerecorded message.

¹⁵ See Request for Comment, *supra* note 3, at ¶¶ 60, 61.

¹⁶ Comments of Comcast Corporation, CG Docket 17-59 and WC Docket No. 17-97, at 3 (filed Dec. 10, 2021), *available at* [https://ecfsapi.fcc.gov/file/121099934097/Comcast%20Comments%205th%20Robo-4th%20Auth%20FNPRM%20\(2021.12.10\).pdf](https://ecfsapi.fcc.gov/file/121099934097/Comcast%20Comments%205th%20Robo-4th%20Auth%20FNPRM%20(2021.12.10).pdf) .

¹⁷ See ZipDX Comments, *supra* note 10, at 25.

III. The Commission Should Require Publication of Traceback Information to Equip Providers and Protect Consumers.

The Commission should mandate that traceback information for illegal robocalls and scam calls be publicly available, both to assist service providers and to help consumers protect themselves. At a minimum, where a traceback has been substantiated,¹⁸ the originating caller, the gateway provider (if a foreign-based call), and the first intermediate provider should be publicly disclosed. If the calls are routed into the U.S., then out again, and then in, all those providers that preceded the last entry into the U.S. should be listed.

This information will assist downstream service providers in making determinations about which callers and upstream providers are the riskiest to carry traffic from. It will also assist other businesses in the marketplace who may seek to use a more reputable service for automated notifications to its own customers by filtering out from its consideration those which have triggered tracebacks. Additionally, public disclosure of traceback information would provide State attorneys general and private litigants with more tools for combatting bad actors in court, which also puts more cops on the beat and furthers the intent of the Telephone Consumer Protection Act to foster private enforcement.

Some information about 2021 traceback efforts was made public in the letter from the Industry Traceback Group (ITG) of November 15, 2021, to the Commission.¹⁹ This letter showed that an alarming number of providers had failed to respond to traceback requests. The Commission's 2021 Annual Report to Congress identifies providers that failed to respond to

¹⁸ We would encourage the Commission to consider calls deemed “highly likely” to be live scam or unconsented-to robocalls to be substantiated tracebacks.

¹⁹ See Letter of Joshua M. Bercu and Jessica Thompson, USTelecom, to Marlene Dortch, Federal Commc'ns Comm'n, Enforcement Bureau Requests Information on the Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls, EB Docket No. 20-195 (filed Nov. 15, 2021), *available at* <https://ecfsapi.fcc.gov/file/111572802120/USTelecom%20Letter%20re%20Status%20of%20Private-Led%20Traceback%20Efforts%202021.pdf>.

traceback requests three times or more.²⁰ But neither report identifies providers who failed to respond to one or two traceback requests. Nor does either report identify providers who have repeatedly been found responsible through tracebacks for originating or transmitting illegal calls through their networks. Without information about which providers have already been found to have originated and transmitted calls that were likely illegal, downstream providers have limited means to determine from whom they should accept calls. Moreover, the public—even the consumers who have been victimized by these illegal calls—have no access to this critical information.

There is already a disconnect between the information about illegal calls that the Commission has and enforcement regarding these illegal calls. In the recent 2021 Report to Congress, the Commission listed nearly 50 providers who were non-responsive to three or more traceback requests in 2021.²¹ Of these, at least five foreign-based providers²² and two U.S.-based providers²³ appeared on the same list in the 2020 report.²⁴ Sixty-two providers appear on both the 2020 and the 2021 lists as refusing at least one traceback request.²⁵

²⁰ Federal Commc'ns Comm'n, Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information (Dec. 22, 2021), *available at* <https://www.neca.org/docs/default-source/wwpdf/public/122821robocall.pdf> [hereinafter 2021 Report] at 35.

²¹ *Id.* at 35.

²² For example, Lexico Telecom LTD, Marketing Maestros, Sumco, Trivia Software Technologies. Lexico, in particular, was non-responsive to 18 traceback requests per the Commission's 2020 Report and non-responsive to 27 per its 2021 Report.

²³ For example, Teli Communications and Vitcomm. *See* Federal Commc'ns Comm'n, Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information (Dec. 23, 2020), *available at* <https://docs.fcc.gov/public/attachments/DOC-368957A1.pdf> [hereinafter 2020 Report].

²⁴ *See* <https://www.neca.org/docs/default-source/wwpdf/public/122821robocall.pdf> <https://docs.fcc.gov/public/attachments/DOC-368957A5.xlsx> at tab "2020 NR Providers."

²⁵ *Compare id* at tab "non-Responsive" *with* the 2021 Report, *supra* note 20, at 32-34. Sixty-two names appear on both lists, including many of the names listed above (*see* notes 22 and 23, *supra*), meaning that sixty-two providers that refused at least one traceback request in 2020 did so again in 2021, nearly all of whom did not provide a reason for their refusal.

More importantly, because of public information available from state enforcement efforts against persistent providers of illegal calls, we know that some providers persist in transmitting illegal traffic even after repeated warnings. For example, in a comprehensive complaint filed this year in federal court, the Indiana Attorney General alleged that the provider Piratel operates a VoIP business that transmitted foreign robocalls²⁶ that it “knew or consciously avoided knowing were illegal,” “despite multiple warnings from third-parties about the illegal calls and multiple warnings.”²⁷

Yet, that type of information is not included in any of the information made public by either the ITG or the Commission. No providers are named in the ITG letter. The Commission’s Report to Congress has a list of providers who were *recipients* of traceback requests, but it does not explain which providers were originating providers, gateway providers, first intermediate providers, or those farther down the call path.²⁸ The Indiana Attorney General’s complaint tells us that Piratel provided gateway or originating services to the foreign callers making illegal calls. Yet, in the Report to Congress, Piratel is reported only in the list of providers who were recipients of traceback requests.²⁹ Simply appearing on the list of providers who have responded to tracebacks does not provide any valuable information, as even highly compliant terminating providers (such as AT&T and Verizon) were recipients of traceback requests, as terminating providers. The critical information that the Commission should make public is a list of providers who were originating or gateway providers, as well as the first intermediate providers, who were asked to traceback their calls.

²⁶ See Complaint for Civil Penalties, Permanent Injunction, Other Equitable Relief, and Demand for Jury Trial, *Indiana v. Startel Comm’n L.L.C.*, No. 3:21-cv-00150-RLY-MPB, 2021 WL 4803899, at ¶ 50 (S.D. Ind. Oct. 14, 2021).

²⁷ *Id.* at ¶¶ 45-48.

²⁸ 2021 Report, *supra* note 20, at 26.

²⁹ See *id.*

There is nothing to prevent the Commission from publishing the names of originating, gateway, and initial intermediate providers who were the recipients of repeated traceback requests. The TRACED Act, which was passed to protect consumers from these illegal calls,³⁰ gives the Commission the explicit authority to report on the voice service providers who either originated and transmitted the illegal calls:

e) List of Voice Service Providers.--The Commission may publish a list of voice service providers and take appropriate enforcement action based on information obtained from the consortium about voice service providers that refuse to participate in private-led efforts to trace back the origin of suspected unlawful robocalls, and other information the Commission may collect about voice service providers that are found to originate or transmit substantial amounts of unlawful robocalls.³¹

The ITG knows who these offending providers are. The offending providers themselves know who they are because they are repeatedly asked for tracebacks of calls originated by or transmitted through their networks. It is not clear whether Commission knows who they are.³² But the Commission has the authority, and the mandate, to find out, and to inform the world of who they are.

³⁰ Six Senate and House leaders said at the TRACED Act's passage: "It's time to put Americans back in charge of their phones." Press Release, House Comm. On Energy & Commerce, House & Senate Announce Agreement on Anti-Robocall Bill (Nov. 15, 2019), *available at* <https://energycommerce.house.gov/newsroom/press-releases/house-senate-announce-agreement-on-anti-robocall-bill>. Senator 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." Press Release, Ed Markey, U.S. Senator for Massachusetts, Senate Overwhelmingly Approves Thune, Markey Bill to Crack Down on Annoying, Illegal, and Abusive Robocalls (May 23, 2019), *available at* <https://www.markey.senate.gov/news/press-releases/senate-overwhelmingly-approves-thune-markey-bill-to-crack-down-on-annoying-illegal-and-abusive-robocalls>.

³¹ See TRACED Act, Pub. L. No. 116-105, § 13(e), 133 Stat. 3274 (2019).

³² Despite receiving more complaints in every category over the same time period last year, the Commission did not report any new citations and only reported one new Notice of Apparent Liability as compared with its reported activities for 2020. Compare the lower-most row appearing at page 5 of the 2021 Report, *supra* note 20, with the same appearing at page 4 of the 2020 Report, *supra* note 23. Compare also 2020 Report, *supra* note 23, at 4-7, with 2021 Report, *supra* note 20, at 5-7. "John M. Burkman, Jacob Alexander Wohl, and J.M. Burkman & Associates LLC" appears to be the only NAL issued in 2021 that was not already in progress in 2020.

Maintaining the secrecy about which providers have repeatedly been the subject of tracebacks deprives downstream providers of the information they need to identify the providers from which they should avoid accepting calls. It also means that consumers who want to enforce the TCPA remain in the dark about the callers and the providers who have facilitated the illegal calls, leaving them with few meaningful ways of obtaining relief for the continuing illegal activity.

The Commission asked “[s]hould we make clear that a gateway provider will not be liable for failing to block where the information is not readily available ...?”³³ The answer to this should absolutely be “No.” The Commission should take action so that the information is always readily available, and providers have no excuse for accepting illegal calls and passing them through to consumers.³⁴

IV. Effective Delisting from the Robocall Mitigation Database Should Automatically Follow Repeated Tracebacks Against Providers, Failure to Respond to Tracebacks, and Other Indicia of Non-Compliance.

The Commission’s use of the Robocall Mitigation Database (RMD) to enforce compliance with the requirement to report the provider’s use of STIR/SHAKEN or alternative authentication methodologies was a brilliant idea. That same mechanism should also be used to combat scam calls and illegal robocalls found after tracebacks, and to require compliance with traceback requests.³⁵

³³ Request for Comment, *supra* note 3, at ¶ 78.

³⁴ As noted in the ZipDX Comments, *supra* note 10, at 21 (“Improving traceback transparency is a simple non-technical enhancement that can be implemented immediately.”).

³⁵ See USTelecom Comments, *supra* note 10, at 9 (“In addition, the Commission should – informed by industry traceback results – actively audit the database to ensure that foreign service providers that are indirectly sending traffic to the United States through intermediate foreign providers are adhering to their RMD commitments. It should then actively take appropriate action (including industry notification) to remove any registrant that does not comply with that registrant’s certification. The need to ensure compliance with RMD obligations are administrative and investigative functions the Commission itself must perform.”); ZipDX Comments, *supra* note 10, at 21 (“To the extent that the designated consortium is unable or unwilling to proactively share time-critical traceback details, the Commission should routinely obtain that information from them and post it for everyone’s benefit.”); Comments of YouMail, Inc., CG Docket No. 17-59 and WC

The Commission’s use of the RMD requires that a provider have a mitigation methodology, and it requires that the provider inform the Commission about that methodology. Failure to have a methodology or failure to inform the Commission leads to automatic effective delisting,³⁶ which means that downstream providers are prohibited from accepting calls from the delisted provider.³⁷ But there is no current requirement imposed by the Commission that the mitigation methodology listed actually be effective in *preventing* the transmission of illegal calls.

The world of consumer law offers two good analogies that illustrate the importance and benefits of requiring an effective methodology. On the one hand is the legal requirement under the Fair Credit Billing Act, that banks are responsible for losses resulting from fraud, and even error.³⁸ This requirement has led to that industry’s development of aggressive and innovative solutions that protect both consumers and the banks from the losses they would bear if the banks followed sloppy security practices. In comparison, under the Fair Credit Reporting Act (FCRA), credit reporting agencies can avoid all liability for mistakes in consumers’ credit reports by simply having “reasonable procedures” in place to address consumer complaints.³⁹ If the credit reporting agency has

Docket No. 17-97, at 10 (filed Dec. 8, 2021), *available at* <https://ecfsapi.fcc.gov/file/1208466000554/Comments%20of%20YouMail%20Inc.-Docket%20Nos.%20CG17-59%20and%20WC17-97.pdf> [hereinafter YouMail Comments] (“YouMail believes that auditing and analysis of calling patterns needs to be supplemented by research of both public and private information providing evidence that specific call sources are committing harm to the public. This can be done through periodic ‘content sampling’ of robocalls and ‘complaint boards.’ This information can be found on numerous robocall registries, such as 800notes, Numberguru and YouMail.”).

³⁶ ZipDX Comments, *supra* note 10, at 24 (“We would note that ‘delisting’ should not actually constitute complete removal from the database; rather, an entry should be retained so that it is clear to all others that the problematic provider has been explicitly designated as such. This will ensure that if (when) the problematic provider attempts to shift their traffic to a new downstream, that downstream will become aware of the situation before enabling the traffic.”).

³⁷ See Federal Comm’n’s Comm’n, Public Notice, Wireline Competition Bureau Reminds Providers of September 28 Blocking Deadline, WC Docket No. 17-97 (Sept. 28, 2021), *available at* <https://docs.fcc.gov/public/attachments/DA-21-1218A1.pdf>.

³⁸ See 15 U.S.C. § 1643.

³⁹ 15 U.S.C. § 1681(b).

procedures that are reasonable but not particularly effective, it still has no liability for consumers' losses, so it has little incentive to monitor the effectiveness of its procedures and improve them. As a result, while complaints about errors in credit reports account for 50% of all the complaints to the Consumer Financial Protection Bureau last year, fewer than 2% of consumers were able to obtain corrections in their reports.⁴⁰ As the CFPB recently noted, this is clearly inadequate.⁴¹ The comparative effectiveness of these two consumer protection laws presents a telling parallel to the Commission's reliance on the robocall mitigation database as a means of stopping illegal calls. In their comments, both CTIA⁴² and USTelecom⁴³ encourage the Commission to identify and act on insufficient robocall mitigation programs, and we strongly agree.

The continued presence of known bad actors—who have been found by the Commission to have originated illegal calls—on the RMD exemplifies the problem with the current regime. Just like the inadequate requirement in the FCRA for credit reporting agencies to simply have a procedure to correct errors, the Commission's vague threats of removal from the database at some point in the

⁴⁰ See Press Release, Consumer Fin. Prot. Bureau, CFPB Releases Report Detailing Consumer Complaint Response Deficiencies of the Big Three Credit Bureaus (Jan. 5, 2022), *available at* <https://www.consumerfinance.gov/about-us/newsroom/cfpb-releases-report-detailing-consumer-complaint-response-deficiencies-of-the-big-three-credit-bureaus/>.

⁴¹ *Id.*

⁴² See Comments of CTIA, CG Docket No. 17-59 and WC Docket No. 17-97, at 3 (filed Dec. 10, 2021), *available at* <https://ecfsapi.fcc.gov/file/12101064726561/211210%20FINAL%20CTIA%20Gateway%20Provider%20NPRM%20Comments.pdf> (“The Commission should also continue to leverage existing tools that have proven effective in helping protect U.S. networks from illegal foreign-originated robocalls, while maintaining the careful balance between fighting illegal robocalls and protecting legitimate calls under the robocall abatement framework already deployed. This should include continuing enforcement against bad actor providers that are not mitigating illegal foreign robocalls and requiring updates to those providers’ robocall mitigation programs that are deemed insufficient, as well as encouraging ongoing participation by all providers in traceback, know-your-customer, call blocking, call authentication, and other efforts to protect consumers.”).

⁴³ See USTelecom Comments, *supra* note 10, at 9 (“The need to ensure compliance with RMD obligations are administrative and investigative functions the Commission itself must perform.”). See also *id.* at 8 (“The Commission can and should take action to ensure that RMD filings are proper and valid, and take action when they are not.”).

future are clearly inadequate. The Commission should make it clear that it will delist providers whose dumping of illegal calls into the American telephone network is evidenced by repeated tracebacks. Similarly, a single failure of a provider to respond to a traceback request should cause automatic delisting from the RMD. The Commission's failure to hold providers accountable for consumer losses is essentially opting for a Fair Credit Reporting Act accountability model rather than the much more effective Fair Credit Billing Act model.

V. The Commission Should Treat Ongoing Provider Non-Compliance as Complicity with Bad Actor Callers.

We could not agree more with Commissioner Starks' observation: "illegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it."⁴⁴ Unless all of the providers who know or should know that the calls they are transmitting are illegal are punished, other efforts to prevent illegal foreign calls through gateway providers are unlikely to succeed.

The Commission has already outlined several actions by providers that are evidence of failing to adequately mitigate bad calls. These include failing to comply with its own stated mitigation program, failing to respond to tracebacks in a timely and thorough manner, serving as the originator for unlawful robocall campaigns, failing to effectively mitigate traffic when notified by the Commission, failing to take reasonable measures to implement an effective call authentication framework, and failing to adopt affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls.⁴⁵ To these, we would add being subject to

⁴⁴ *In re* Call Authentication Trust Anchor, WC Docket No. 17-97 (Sept. 30, 2021) (Statement of Comm'r Geoffrey Starks), available at <https://docs.fcc.gov/public/attachments/FCC-21-105A3.pdf>.

⁴⁵ See *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, CG Docket No. 17-59, 35 FCC

more than one substantiated traceback request. Any one of these actions should result in a provider's removal from the robocall mitigation database and downstream providers being required to block all traffic from the offending provider.

We also agree with YouMail that it is appropriate for the FCC to impose a “know or should have known standard” on providers.⁴⁶ The clock must start when the provider has reason to know that it is trafficking in illegal calls, not when the Commission comes knocking.

In addition to moving much more swiftly to bar non-responsive and non-compliant providers from the RMD and facilitating public and private enforcement by making tracebacks public, the Commission should articulate that providers will be liable for violations of any relevant law, with a forfeiture assessed by the FCC of no less than \$0.10/call. This would make it financially risky for providers to accept calls from providers who are likely to break the law. If providers are equipped with information about who is risky, through public disclosure of substantiated tracebacks, they can make more informed decisions about whose traffic to carry and whose to block or to let other providers assume the risk of carrying.

VI. Conclusion

We appreciate the opportunity to offer comments on how the Commission can better protect the American telephone network through its regulation of gateway providers, and we are encouraged by the comments of the industry on this docket urging for more immediate action on this issue. We urge the Commission to impose a general duty to mitigate on gateway providers, and

Rcd 7614, 7627, at ¶¶ 35-45 (July 16, 2020), *available at* <https://docs.fcc.gov/public/attachments/FCC-20-96A1.pdf>.

⁴⁶ See YouMail Comments, *supra* note 35, at YouMail at 4 (“The standard ‘knew or should have known’ based on the facts is an appropriate standard for the FCC to use as well. Indeed, the Commission has done so in several Telephone Consumer Protection Act (“TCPA”) cases.”).

on all providers, that requires affirmative, effective efforts, to hold providers liable for consumer losses resulting from scam calls and illegal robocalls, and to require public disclosure of certain substantiated traceback information. We reiterate that providers should not sit back and wait until the Commission confronts them with their inadequate robocall mitigation program—they should be held to a “know or should have known” standard to comply with the Commission’s rules and align their business practices with the goal of facilitating only legitimate calls.

Respectfully submitted, this the 10th day of January 2022, by:

Chris Frascella
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036
frascella@epic.org

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