Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of		
Improving the Effectiveness of the Robocall Mitigation Database	)	WC Docket No. 24-213
Amendment of Part 1 of the Commission's Rules, Concerning Practice and Procedure, Amendment of CORES Registration System	)	MD Docket No. 10-234

Comments on the
Notice of Proposed Rulemaking (WC Dkt. No. 24-213 and MD Dkt. No. 10-234)
Issued on August 8, 2024

Comments of

Electronic Privacy Information Center
Public Knowledge
National Consumers League

Submitted October 15, 2024

By:
Chris Frascella
Matt Contursi
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036

Peter Gregory
Public Knowledge
1818 N St, NW, Suite 410
Washington, D.C. 20036

Eden Iscil
National Consumers League
1701 K St, NW, Suite 1200
Washington, D.C. 20006

Summary

Robocalls continue to menace consumers at a rate of billions of calls every month, with tens of billions of dollars in annual losses due to scams alone—not to mention illegal telemarketing calls and other unwanted nuisance calls. The Federal Communications Commission (FCC or Commission) in this Notice of Proposed Rulemaking (NPRM) outlines promising proposals for improving voice service provider and intermediate provider ("provider") obligations in its Robocall Mitigation Database (RMD) and the Commission's related enforcement powers.

Our recommendations within this comment reflect the Commission's interests in bolstering the RMD to be a resource that holds providers accountable to their own STIR/SHAKEN implementation plans and brings meaningful enforcement of the TRACED Act. While we support the Commission's proposals for expedited enforcement of facially deficient RMD entries, the Commission should prevent these entries from being filed in the first place, and it has the imperative and the authority to define "facially deficient" more broadly than it currently proposes. And while we support the Commission's proposals for enforcement penalties for failing to comply with updates within 10 days, along with greater personal accountability and security measures, the Commission should also require annual certifications that this update requirement has been fulfilled. We unequivocally support the Commission's proposals for remittance fees, and we encourage the Commission to continue to pursue more intensive investigations of less obvious non-compliance by complicit and complacent providers facilitating illegal robocall campaigns.

The RMD holds a number of deficient entries, such as entries lacking basic contact information for listed providers (like a business address or phone number), entries with no

information as to the status of the provider's STIR/SHAKEN implementation, and entries completely lacking details of the provider's robocall mitigation plan. We also anticipate, as this NPRM does as well, that there are entries that are not facially deficient but do not accurately reflect a provider's business practices or do accurately reflect practices that are insufficient to effectively mitigate robocalls. A deficient entry within the RMD is a vulnerability. The RMD has a dual purpose: (1) to keep the Commission and the public informed on what a provider is doing to curb the tide of illegal robocalls and (2) to hold providers accountable to their plans. Deficient entries within the RMD, just like deficient robocall mitigation itself, cannot be tolerated and we are pleased with the steps the Commission is taking in this Notice.

Table of Contents

I. Introduction

The Electronic Privacy Information Center (EPIC)[1], along with Public Knowledge[2] and the National Consumers League,[3] ("Consumer Advocates") file these comments regarding the issues raised in the Notice of Proposed Rulemaking (NPRM) regarding the Robocall Mitigation Database (RMD) and CORES Registration Process on how to ensure voice service providers and intermediate providers ("providers") are submitting to the RMD with diligence and accuracy.[4] The Federal Communications Commission (FCC or Commission) has already taken steps to deter providers from being complacent or complicit with bad actors, and this NPRM represents another step in the right direction. However, the Commission's proposals still do not go far enough because they do not adequately capture what constitutes a facially deficient RMD entry. Because of the severe damage illegal robocall campaigns can cause—more rapidly even than traditional regulatory and enforcement mechanisms can respond—swift

[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] **Public Knowledge** is a non-partisan, non-profit consumer rights organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works. It has worked for many years to promote telecommunications policies that protect consumers, and has filed comments to the Federal Communications Commission (FCC) on proposals supporting the protections of the Telephone Consumer Protection Act (TCPA). https://publicknowledge.org.

[3] The **National Consumers League** is a non-profit, non-partisan consumer advocacy organization representing consumers and workers on marketplace and workplace issues since its founding in 1899. Headquartered in the District of Columbia, NCL provides government, businesses, and other organizations with the consumer's perspective on concerns including child labor, privacy, food safety, telecommunications, and medication information. https://nclnet.org.

[4] *In re* In the Matter of Improving the Effectiveness of the Robocall Mitigation Database, Amendment of Part 1 of the Commission's Rules, Concerning Practice and Procedure, Amendment of CORES Registration System, Notice of Proposed Rulemaking, WC Dkt. No. 24-213, MD Dkt. No. 10-234 (Rel. Aug. 8, 2024), https://docs.fcc.gov/public/attachments/FCC-24-85A1.pdf [hereinafter "RMD NPRM"].

enforcement is necessary to adequately protect consumers. The Commission must empower entities to flag facially deficient RMD entries to enable prompt enforcement and an efficient RMD mechanism.

In **section II**, we briefly outline the continuing harms that consumers face from illegal call campaigns as well as actions the Commission has taken to improve the RMD to prevent harm.

In **section III**, we support the Commission's reiteration and enforcement of the fundamental eligibility requirements for the RMD, including basic contact information, which many entries currently fail to satisfy despite longstanding notice from the Commission that this information is necessary.

In **section IV**, we support the Commission's proposed 10-day RMD update obligation but urge the Commission to require additional updates for particular triggering events and annual certifications from providers.

In **section V**, we support the Commission's use of remittance fees to incentivize compliance with its proposed measures to improve the RMD.

In **section VI**, we support the Commission's use of an expedited process to suspend facially deficient RMD entries, but we urge the Commission to include factors such as non-responsiveness to traceback requests and continually connecting illegal calls as indicia of facially deficient RMD entries.

In **section VII**, we offer considerations for the Commission as it develops its lengthier adjudicative process for defective RMD entries that are not necessarily facially deficient.

II. Consumers continue to bear the brunt of illegal robocall operations, although the Commission is making improved use of its tools to remedy this.

Phone subscribers are still plagued by illegal calls at a staggering rate. There were more than 4.5 billion robocalls sent in September 2024; more than one billion of those were scams (an estimated 20% of the 4.5 billion robocalls were scam robocalls), and approximately 1.5 billion of those were telemarketing robocalls (an estimated 33% of the 4.5 billion), which can also represent harmful illegal campaigns.[5] With the exception of December 2023, in which there were an estimated more than 791 million scam robocalls,[6] Consumer Advocates were not able to identify a month in which there were fewer than 1 billion monthly scam robocalls since the release of EPIC and NCLC's report in July 2022.[7] In its most recent report, TrueCaller estimated that more than $25 billion dollars was lost to scam robocalls in 2023.[8]

As the Commission has recognized through its partnerships with state Attorneys General[9] and other law enforcement,[10] the RMD is meant to be a central resource in mitigating unwanted

---

[5] *See* YouMail Robocall Index, https://robocallindex.com/ (last visited Oct. 15, 2024). YouMail has noted that "calls initially viewed as telemarketing are eventually recognized as illegal telemarketing or scam calls, so it's important to measure the overall quantity of scam and spam calls combined." PR Newswire, Robocalls Top 50.3 Billion in 2022, Matching 2021 Call Volumes Despite Enforcement Efforts (Jan. 5, 2023), https://www.prnewswire.com/news-releases/robocalls-top-50-3-billion-in-2022–matching-2021-call-volumes-despite-enforcement-efforts-301714297.html. The universally-reviled calls selling auto warranties—targeted by the Ohio Attorney General and the Commission are considered telemarketing calls, not outright scam calls, *see, e.g.*, Press Release, Yost Files Suit Alleging Massive Robocall Scheme – FCC Joins Fight in Related Action (Jul. 7, 2022), https://www.ohioattorneygeneral.gov/Media/News-Releases/July-2022/Yost-Files-Suit-Alleging-Massive-Robocall-Scheme-F; conversation with Mike Rudolph, CTO, YouMail, Aug. 29, 2022.

[6] 21% of 3,769,595,200 is approximately 791.6 million. *See* December 2023 Nationwide Robocall Data, YouMail Robocall Index, https://robocallindex.com/2023/december.

[7] *See* NCLC and EPIC, Scam Robocalls: Telecom Providers Profit (June 2022), https://epic.org/documents/scam-robocalls-telecom-providers-profit/.

[8] *See* Truecaller, America Under Attack: The Shifting Landscape of Spam and Scam Calls in America at 3-4 (Mar. 12, 2024), available at https://drive.google.com/file/d/1M0J0wO6YqxDzsOizfal-AH_vI8dsyojb/view.

[9] FCC, *FCC-State Robocall Investigation Partnerships*, FCC (Mar. 11, 2024), https://www.fcc.gov/fcc-state-robocall-investigation-partnerships.

[10] *See, e.g.*, 47 C.F.R. § 64.6305(d)(2)(iv) (requiring statement whether filing entity was "subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating

and scam calls. Industry has agreed with this for years.[11] Encouragingly, in its recent orders and continuing with this NPRM, the Commission has steadily sought to improve the RMD.[12]

Authorized in the 2019 TRACED Act and created by the Commission in 2021,[13] the RMD is both a way for the FCC to monitor compliance with STIR/SHAKEN implementation and ensure that providers are connecting to providers who are actively participating in efforts to reduce the torrent of robocalls.[14] Although providers are restricted to only accepting calls from providers registered in the RMD, there are known issues with both the quality of RMD records

---

illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description").

[11] *See, e.g.*, Comments of USTelecom – The Broadband Association, CG Docket No. 17-59 and WC Docket No. 17-97, at 2 (filed Dec. 10, 2021), https://www.fcc.gov/ecfs/search/search-filings/filing/12101593911611 ("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*); 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."); id. 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").

[12] *See, e.g.*, Public Notice, Wireline Competition Bureau Announces Robocall Mitigation Database Filing Deadlines and Instructions and Additional Compliance Dates (Rel. Jan. 25, 2024), https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf (requiring all providers to file certifications, among other requirements); Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59 (Rel. May 19, 2023), https://docs.fcc.gov/public/attachments/FCC-23-37A1.pdf [hereinafter "Seventh Report and Order in CG 17-59 (2023)"] (requiring all providers to respond to tracebacks and implement Know Your Upstream Provider (KYUP) programs, among other requirements); Sixth Report and Order in CG Docket No. 17-59, Fifth Report and Order in WC Docket No. 17-97, Order on Reconsideration in WC Docket No 17-97, Order, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 at ¶ 40 (Rel. May 20, 2022), https://docs.fcc.gov/public/attachments/FCC-22-37A1.pdf [hereinafter "Sixth Report and Order in CG 17-59 (2022)"] (noting that a certification that describes an ineffective program is deficient).

[13] *See* Public Notice, Wireline Competition Bureau Announces Opening of Robocall Mitigation Database and Provides Filing Instructions and Deadlines , DA 21-454 (Apr. 21, 2021), https://docs.fcc.gov/public/attachments/DA-21-454A1.pdf.

[14] *See, e.g.*, Media Release, FCC Robocall Response Team Has Taken Enforcement Actions, Built Nationwide Partnerships, and Proposed Innovative New Policies to Combat Scam Robocalls, DOC-384793A1 (Jun. 30, 2022), https://docs.fcc.gov/public/attachments/DOC-384793A1.pdf.

and the slow process for removing facially deficient records.[15] In 2022, the Commission focused its efforts to improve the RMD for gateway providers.[16] In 2023, it released its Sixth Caller ID Authentication Report and Order, which updated RMD requirements for all providers.[17]

These recent implementations have not eliminated illegal calls, which still plague subscribers at a staggering rate. But we are optimistic that the Commission's proposed changes, enhanced by our recommendations below, may help to further mitigate the harm to consumers.

III. The Commission should not permit a provider to submit an RMD entry without including basic information.

We urge the Commission to prevent an RMD entry from being created in the first instance without the basic information the Commission has required since March 2023,[18] as this proactive prevention would be more effective and efficient than enforcement after the fact.[19] Although this would not prevent filings containing meaningless information, it would prevent incomplete filings from being added to the database.

---

[15] *See, e.g.*, Comments of EPIC and NCLC, *In re Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 at 14-27 (Aug. 17, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/10817350228611 [hereinafter "EPIC NCLC 2022 7FNPRM Comment"] (arguing for automatic suspension from the RMD); Comments of EPIC and Consumer Action, *In re Numbering Policies for Modern Communications; Telephone Number Requirements for IP-Enabled Service Providers; Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 13-97; 07-243; 20-67 at 4 fn. 18 (Nov. 29, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1130061407794 ("EPIC maintains that [the RMD suspension] process gives bad actors too many and prolonged opportunities to continue abusing resources and scamming called parties.").

[16] *See* Sixth Report and Order in CG 17-59 (2022), *supra* note 12.

[17] *In re* Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Dkt. No. 17-97 (Rel. Mar. 17, 2023), https://www.govinfo.gov/content/pkg/GPO-FCC-Rcd-V38No3/pdf/GPO-FCC-Rcd-V38No3.pdf [hereinafter "Sixth Report and Order in WC 17-97 (2023)"].

[18] *See* RMD NPRM at ¶ 7 (citing to Sixth Report and Order in WC 17-97 (2023), among other citations).

[19] Proactive prevention would be "faster" than the expedited *ex post* measures the Commission proposes. *See* RMD NPRM at ¶ 40 (citing to Sixth Report and Order in WC 17-97).

Upon accessing the database on October 15, 2024, there were 9,333 total entries,[20] of which 609 claimed their STIR/SHAKEN implementation status was "N/A";[21] 601 did not offer a contact phone number;[22] and 423 entries without a phone number also did not have any other entries or reported aliases in other databases.[23] While these may represent less than 7% of all records in the database, these are entries that are egregiously noncompliant with the standards for inclusion in the RMD.[24] Providers have received ample notice about and have had ample time to comply with the Commission's requirements for the RMD. Omitting such fundamental information obstructs transparency and accountability measures. The Commission should suspend providers who still fail to include this basic information today, as they are facially deficient more than eighteen months after the Commission updated its requirements. Going forward, the Commission should not permit providers to submit an RMD entry without including this information, and should implement its expedited process for facially deficient entries when the information provided in an RMD entry is present but is clearly inaccurate.

[20] Robocall Mitigation Database, FCC, https://fcc.gov/robocall-mitigation-database (last visited Oct. 15, 2024).

[21] *Id.* The database was downloaded as a CSV and analyzed in Microsoft's Excel; filtering was applied to the dataset unaltered to select for portions where the variable "implementation" equaled "N/A"

[22] *Id.* Filtering was applied to the dataset unaltered to select for portions where the variables "contact_name" and "contact_phone" equaled "N/A"

[23] *Id.* Filtering was applied to the dataset unaltered to select for portions where the variables "other_frns", "other_db_names", "previous_dba_names", "contact_name" and "contact_phone" equaled "N/A", "None", "No", or "Noe" or other variants (e.g. "Ninguno"). We also note that in at least one instance, the name listed under "other db names" did not appear elsewhere in the RMD (e.g. "Appalachian Telecom, Inc." listed "ATI Broadband" as an alternative name, with no other record of ATI Broadband appearing in the RMD)—meaning there was no clear alternative record in which to find the information missing from that company's entry.

[24] We recognize that some of these may have been imported from other databases and not filed by the company directly into the RMD. However, per 47 C.F.R. § 64.6305(g), providers know that their calls will not be transmitted unless they are in the RMD and so they are on notice to check their RMD entry, even if they did not themselves create it in the RMD directly.

IV. The obligation to update an RMD entry within 10 days should be enforceable, matched by an obligation to certify an entry's accuracy annually, and more secure.

The undersigned consumer advocates strongly support the Commission's efforts to enforce the requirements that a provider update their RMD entry within 10 days of a change. However, we urge the Commission to clarify that changes to any required information—not just changes to contact information—must trigger the 10-day update deadline, and to additionally require that companies must certify annually that any necessary updates were timely made. We also support the Commission's proposal to issue the person within the company responsible for addressing robocall mitigation-related matters a PIN to manage the business' RMD entry and to enable multi-factor authentication (MFA) for their account. The Commission has already required these timely updates as a transparency measure and now merely proposes putting more direct enforceability behind them. As noted above, transparency and accountability are essential in effectively combatting robocalls. Moreover, the ability of good actors in the ecosystem to quickly reach responsible company officers impacts the industry's ability to respond to illegal call campaigns and facilitates holding bad actors responsible.

As the Commission noted,[25] 47 C.F.R. § 64.6305 requires each provider to update its RMD entry within ten days with any changes regarding not only contact information, but other information as well: the status of its STIR/SHAKEN implementation; reasonable steps taken to avoid originating (or carrying or processing, depending on the carrier's role) illegal robocall traffic, including how it complies with 'Know Your Upstream Provider' (KYUP) obligations; the analytics system it uses to identify and block illegal traffic, including the name of any vendors

[25] *See* RMD NPRM at ¶ 10 n. 49.

used; whether the provider has been subject to any action or investigation (but not mere inquiry) related to illegal robocalls, spoofing, or deficient robocall mitigation program descriptions or RMD certifications; and its commitment to responding to tracebacks within 24 hours. However, in its NPRM, the Commission places heavy emphasis on the importance of updating contact information.[26] We encourage the Commission to clarify that the enforceable requirement to update an RMD entry within 10 days is not limited to contact information updates.

We also believe this obligation should be matched with greater accountability given the importance of the RMD. In addition to the 10-day update requirement, providers should be obligated to confirm annually that their RMD registry information has been accurately updated, in accordance with the above additional requirements, within the last year. The burden associated with this additional task is minimal, and it would promote periodic attention to this requirement from providers.

If a provider fails to confirm its information during a designated check-in period, we suggest a structured enforcement process. Initially, the provider should receive a warning letter, accompanied by a 30-day deadline to log into their CORES account and confirm that their information remains current.[27] If the provider fails to meet this deadline, they should be suspended from the database. These actions are within the FCC's scope of authority, and this simple, yet effective, structured enforcement process is commonplace with other US agencies.[28]

---

[26] *See, e.g., id.* at ¶¶ 10, 13, 18.

[27] By analogy, the Commission allows 30 days for providers to comply with Final Determination Orders under 47 C.F.R. 64.1200(n)(3).

[28] This is consistent with carriers' obligations to file Customer Proprietary Network Information certifications annually in supplement to more rapid breach notification requirements. *See, e.g.,* FCC Enforcement Advisory No. 2024-01, DA 24-125 (Rel. Feb. 9, 2024), https://docs.fcc.gov/public/attachments/DA-24-125A1.pdf. Looking to how other federal agencies handle self-

Secure access for creating and updating RMD entries is also important to ensuring accountability. We strongly support the assignment of a secure PIN to a company representative who is obligated to be responsive to and responsible for their business's entry within the RMD. Requiring a company officer to maintain a unique PIN for the company's account establishes a clear chain of responsibility within each provider organization. This accountability mechanism ensures a person to whom the Commission, ITG, or others can reliably get into contact with if they have any questions or concerns regarding the provider.

Assigning the responsibility of maintaining a PIN to a corporate officer links the performance and compliance of the provider directly to an individual with authority within the organization.[29] In creating effective governance, data privacy and security scholars have noted that accountability is effective when there are three key elements present: (1) transparency (having access to information about commitments regarding the promised function), (2) answerability (able to have someone to request information about actions an entity takes), and (3) enforceability (being able to sanction an actor is if fails to meet certain standards).[30]

---

reporting as a form of oversight, the Centers for Disease Control (CDC) in administering the PulseNet Laboratory Network, regularly requires participating public health labs to submit not only quality assurance documents on their molecular detection capabilities, but also submit annual surveys on information pertaining to the lab and their employed methodologies. *See* PulseNet Quality Assurance/Quality Control (QA/QC) Manual at 32 (May 9, 2005) https://pulsenetinternational.org/assets/PulseNet/uploads/QAQC/PulseNet%20QAQC%20ManualNovember18_2010_Pt1.pdf (requiring an annual survey summarizing a fall and a spring round of proficiency testing).

[29] We expect that a company may seek to authorize multiple employees to use the designated person's PIN. We do not take a position on this, but the Commission should not excuse the designated individual nor the company as a whole from enforcement of the company's obligations to ensure its RMD filing is accurate and complete, including timely updates, if multiple employees are given access to this information.

[30] Daniel J. Solove, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014) https://columbialawreview.org/content/the-ftc-and-the-new-common-law-of-privacy/. In *Common Law of Privacy*, Solove argues why the Federal Trade Commission (FTC) can act as an effective regulator for data privacy through holding for-profit companies accountable for what they claim in their own privacy policies. FTC achieves this governance through leveraging their enforcement powers against companies advertising their services in a deceptive manner. This external enforcement leads companies to be accountable to what they claim within their own privacy policies, leading to a quasi self-regulatory environment for data privacy.

Obligating an officer of the company to be responsible for their RMD entry satisfies all three of these elements (the state of a company's RMD entry is publicly accessible, an agent of the company will be solely responsible for amending the entry, and there are actions the FCC can take against the company or the officer directly if they fall out of compliance). This not only increases internal oversight but also encourages proactive and continuing compliance with FCC regulations. Officers are more likely to ensure the company's actions align with the law if they know they are personally associated with the integrity of the registration process and liable for any violations.[31] By letting companies identify the person directly responsible for their RMD entry, the FCC can enhance incentives for providers to comply with their obligations and strengthen the intended impact of the RMD. Lastly, we support the incorporation of multifactor authentication (MFA) when it comes to accessing a portal to edit a business's own RMD entry. Enhanced security would only further solidify the integrity of the RMD and other associated systems, ensuring that providers' accounts remain protected.

A crucial element of maintaining a healthy telecommunications ecosystem is knowing which providers are trustworthy and performing their roles responsibly. Timely updates promote transparency and trust, bolstering the integrity of this system.

V. The Commission should collect remittance fees and hold providers liable for connecting calls from providers without valid RMD entries.

We support the Commission charging a fee to attempt to file in the RMD, as this will create financial disincentives to serial noncompliance without creating significant barriers to entry. Remittance fees encourage companies to get their filing right the first time, and increase

[31] Additionally, it increases accountability for the officer involved. *See, e.g.*, 47 U.S.C. § 217.

the costs for repeat offenders with the hope of changing the calculus such that the bad actor opts not to submit another company into the RMD to profit from trafficking illegal calls.[32] EPIC previously supported a bonding requirement in part for this reason—it makes fraud less economical and thus less attractive to bad actors.[33]

We also note that the Commission must do better to incentivize companies to comply with its requirement to not accept traffic from companies suspended from the RMD. While technically its first-of-its-kind action against One Eye was not a removal from the RMD, it was intended to have the same effect.[34] And yet, after its Final Determination Order took effect,[35] at least one provider continued to accept calls from One Eye, evidenced by at least one traceback.[36] Being suspended from the RMD is only a serious deterrent if the penalty is actually enforced.

VI. The Commission should increase enforcement for facially deficient RMD submissions, including non-compliance with traceback requests and continually connecting illegal calls.

The Commission should implement the expedited process it proposes, not only for facially deficient RMD entries as it has already explicitly defined that in this NPRM,[37] but also

[32] *See, e.g.*, Scam Robocalls: Telecom Providers Profit, *supra* note 7 at 12-14.

[33] *See, e.g., id.* at 30; EPIC NCLC 2022 7FNPRM Comment *supra* note 15 at 28-31. One benefit of bonding not present in this proposal however is that bonding also ensures there is money readily available for remedies. *See* EPIC NCLC 2022 7FNPRM Comment at 31.

[34] In re ONE EYE, LLC, Final Determination Order, DA 23-389, FCC, EB Docket No. 22-174 (Rel. May 11, 2024), https://www.fcc.gov/document/eb-issues-final-determination-order-against-one-eye.

[35] June 11, which was 30 days after the release of the May 11 FDO.

[36] FCC, Report, REPORT ON TRACEBACK DATA FOR THE PERIOD OF APRIL 1, 2023 THROUGH JUNE 30, 2023, DOC-397295A1 (2023) https://www.fcc.gov/document/fcc-releases-traceback-transparency-report. Traceback 13726 on pg 12/14, a bank impersonation scam. USTelecom confirmed that the call occurred after the June 11 deadline (Oct. 18, 2023 email).

[37] *See* RMD NPRM at ¶ 40.

for providers who are non-responsive to tracebacks[38] or who continually connect illegal calls.[39] As part of each RMD entry, the company certifies cooperation with traceback efforts.[40] Additionally, where measures repeatedly fail to stop illegal robocall traffic, the company's actions are demonstrably not "reasonable steps" in service of robocall mitigation.[41] As such, a company's deficiencies in traceback response or in actual robocall mitigation should be treated as a facially deficient RMD entry filed by that company.

As noted above, there are many entries in the RMD that should never have been permitted in the first place.[42] As has been noted by the Commission and others, there are entries with flagrantly deficient mitigation plans.[43] One Senator observed:

> [S]o many are thumbing their nose at a requirement with the mitigation plan. Submitting blank documents, documents that are intended to be rude or menus or

---

[38] *See* Comments of EPIC and NCLC, *In re Call Authentication Trust Anchor*, WC Docket No. 17-97 at 17 (Nov. 12, 2021), https://www.fcc.gov/ecfs/search/search-filings/filing/1113003014007 [hereinafter "EPIC NCLC 2021 S/S Comments"] ("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.").

[39] *See, e.g.*, Seventh Report and Order in CG 17-59 (2023), *supra* note 12 at ¶ 36 fn. 83 ("Voice service providers that fail to take available steps to effectively mitigate illegal traffic may be deemed to have knowingly and willfully engaged in transmitting unlawful robocalls. See, e.g., Sumco Panama Operation Order at 1, para. 1; In the Matter Of Urth Access, LLC, Order, EB-TCD-22-00034232, DA 22-1271 at 1, para. 1 (EB 2022) (Urth Access Order)."); *id.* at ¶ 50 ("However, all voice service providers must take effective steps, and if a voice service provider carries or transmits a high volume of illegal traffic that primarily originates from one or more specific upstream providers, the steps that provider has taken are not effective and must be modified for that provider to be in compliance with our rules. We encourage voice service providers to regularly evaluate and adjust their approach so that that it remains effective.").

[40] *See* RMD NPRM at ¶ 8 (citing to 47 C.F.R. § 64.6305(a)(2), (b)(2), (c)(2)).

[41] *See* RMD NPRM at ¶ 8 (citing to 47 C.F.R. § 64.6305(d)(2)(ii), (e)(2)(ii), (f)(2)(ii), and to Sixth Report and Order in WC 17-97).

[42] See section III, *supra*.

[43] *See, e.g.*, Reply Comments of EPIC and NCLC, *in re* Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, CG Docket No. 17-59, WC Dkt. No. 17-97 at 3 fn 5 (Sept. 16, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/1091775446187 (noting that "[j]ust a few examples include the entries for the robocall mitigation plans certified by several providers. Humbolt VoIP and Huffman Telcom Corp. provide blank pieces of paper. VoIP Network, LLC provides a plan that is for another provider. And the plan for USATOLLNA.COM is the Commission's instructions for filing on the database"). The Commission initiated the process for removing twenty providers for deficient filings. *See, e.g.*, FCC Seeks to Remove Companies from Robocall Mitigation Database (Oct. 16, 2023), https://www.fcc.gov/document/fcc-seeks-remove-companies-robocall-mitigation-database; *see also* FCC to Remove Companies from Robocall Database for Non-Compliance (Oct. 3, 2022), https://www.fcc.gov/document/fcc-remove-companies-robocall-database-non-compliance.

> whatever nonsense is also being submitted shows that it's not working, that there's a loophole somewhere that's been created, that there's no attention to the prosecution side if you will or the requirements for the mitigation plan[.][44]

The Commission should treat these as facially deficient entries and remove them under the expedited process it proposes.

The Commission should also apply its expedited removal process to companies that do not respond to traceback requests within 24 hours. By the time a traceback request is filed with an intermediate provider, the damage of the scam call has already happened, and while some may see a single traceback request as a statistical likelihood, multiple traceback requests from a single provider are indicative of larger issues.[45] Cases involving such companies have already resulted in one consent decree, while others are currently being settled with state attorneys general.[46] To date, there has been chronic inefficiency in achieving provider cooperation with

---

[44] Sen. Ben Ray Luján, Protecting Americans from Robocalls, 118th Cong. (2023), S. Comm. on Comm, Science, and Trans., Subcomm. on Commc'ns, Media, & Broadband at timestamp 1:48:36 (Oct. 24, 2023), https://www.commerce.senate.gov/2023/10/protecting-americans-from-robocalls.

[45] EPIC NCLC 2022 7FNPRM Comment *supra* note 15 at 20 ("A single traceback request serves as notice that something is wrong; multiple traceback requests are a claxon alerting providers who originated the calls, or accepted the calls from originating or gateway providers, that they are transmitting volumes of illegal calls.").

[46] *See, e.g.*, Indiana Complaint at ¶ 314 (S.D. Ind. Oct. 14, 2021) ("On July 22, 2020, Piratel's CEO responded to the email, writing: 'We will need to review internally and with USTelecom as to if we are willing to enable your trunk again. We have received 4 tracebacks in 3 weeks which is the most tracebacks we have received from any single customer, much less in the space of time.'"). *See also id*. at ¶ 316 ("Despite receiving four Tracebacks, which alerted them of illegal robocalls, Piratel did not terminate Startel as a client. Quite the opposite, Startel went on to route millions more calls to Hoosiers through Piratel's system, and Piratel continued to collect thousands of dollars from Startel."). As a result of Indiana's lawsuit, Piratel signed a consent decree requiring the payment of $150,000 over five years, as well as injunctive relief including network monitoring, a prohibition on providing services to new Voice Service Provider (VSP) Customers without first engaging in reasonable screening, and the suspension of service to VSP Customers failing to meet certain requirements – without Piratel admitting fault. *See* Consent Decree, Indiana v. Startel Commc'n L.L.C., No. 3:21-cv-00150 (Apr. 6, 2022). *See also* Complaint, State of Vermont v. Bohnett, Case No. 5:22-cv-00069 at 17 ¶ 79 (D. Vt. Mar. 18, 2022) [hereinafter "Vermont AG Complaint"] (noting recipient of 132 traceback requests); Complaint for Injunctive Relief and Civil Penalties, North Carolina *ex rel.* Stein v. Articul8, LLC & Paul K. Talbot, Case No. 1:22-cv-00058 at 30 ¶ 94 (M.D.N.C. Jan. 25, 2022) (noting recipient of 49 tracebacks).

traceback requests, evidenced in the Commission's annual reporting to Congress.[47] Even in its most recent report to Congress (Dec. 2023), the Commission noted no fewer than fifty U.S.-based providers who were non-responsive to 3 or more traceback requests during that year.[48] As the Commission is strategizing improvements to the RMD, it should take into consideration this perennial issue. If it is to effectively eradicate illegal calls, the Commission must make it more costly for providers to flout compliance with traceback requests.

Providers who repeatedly receive traceback requests and do not adjust their practices, or otherwise evidence behavior that suggests they continue to transmit volumes of illegal robocalls, despite all the Commission has said and done over the past several years, should be shut down. Fines serve as a deterrent to non-compliance and ensure that filings are accurate, but they do not fully compel providers to take meaningful action to prevent illegal robocalls, especially where the amount fined or the likelihood of actually having to pay the amount fined is outweighed by

[47] In the Commission's 2021 report to Congress, 123 providers were listed as nonresponsive. Of those 123 providers, 62 were already listed in the Commission's 2020 report to Congress as non-compliant with one or more tracebacks, many of which were U.S. based providers. *See* EPIC NCLC 2022 7FNPRM Comment *supra* note 15 at 21-22 fn. 74-75 (comparing list of United States companies listed in "Non-Responsive" tab of .xlsx file attachments between Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, Attachment A (Dec. 22, 2021), https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2021-congress and Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, Attachment D (Dec. 23, 2020), https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2020-congress).

[48] Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, Attachment A at "Non-Responsive 2023" filtered by Country: United States (Dec. 27, 2023), https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2023-congress [hereinafter "2023 FCC Report to Congress"]. At least five of these providers also appeared in the same list in the Commission's 2022 report. Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, Attachment A at "Non-Responsive 2022" filtered by Country: United States (Dec. 23, 2022), https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2022-congress [hereinafter "2022 FCC Report to Congress"]. This does not take into account foreign providers who appear perennially, and the downstream domestic providers who continue to accept calls from them.

the expected profits.[49] The real challenge lies in obligating providers to actively participate not only in updating their RMD records but also in actual robocall mitigation practices—and to take responsibility for the calls they transmit. Without this obligation, the regulatory framework will remain reactive rather than proactive.[50] To effectively combat robocalls, the Commission must go beyond simply setting up compliance mechanisms. It needs to hold providers accountable for the results of their business practices, particularly in terms of preventing illegal robocalls from entering the call path. It needs to become more costly to accept risky calls.

Providers that repeatedly connect illegal robocalls should face swift consequences, whether they are accepting calls from providers not listed in the RMD, failing to comply with traceback procedures, or are deficient in other regulatory standards. Providers that continually enable illegal robocalls could be categorized as "High-Risk Providers," a designation that would trigger additional scrutiny and suspension from the RMD as we have argued in previous regulatory comments,[51] or could be categorized as C-CIST, as the Commission has previously done.[52] By categorizing these providers, the Commission can focus its enforcement efforts on the worst offenders and protect consumers from the most harmful actors in the system.

---

[49] This dynamic was noted in 2021 by Commissioner Starks: "[I]llegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it."*In re* Call Authentication Trust Anchor, Further Notice of Proposed Rulemaking, WC Docket No. 17-97 (Sept. 30, 2021) (Statement of Comm'r Geoffrey Starks).

[50] EPIC NCLC 2021 S/S Comments *supra* note 38 at 6 ("In 2019, one single intermediary VoIP provider facilitated *hundreds of millions* of calls within 23 days, depriving consumers of "substantial sum[s]" totaling in the hundreds of thousands of dollars, 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.") (internal citations omitted).

[51] EPIC NCLC 2022 7FNPRM Comment *supra* note 15 at 14-21.

[52] Fact Sheet, Fed. Commc'ns Comm'n, Consumer Communications Information Services Threat (C-CIST) Designation (May 13, 2024), https://www.fcc.gov/document/fcc-classifies-repeat-robocall-bad-actor-first-c-cist.

VII. The Commission should continue to investigate and bring enforcement actions for less obviously deficient RMD entries.

We also support the Commission's efforts to identify less obviously non-compliant providers.[53] There are indicia beyond the facially deficient measures listed in section VI above that a provider needs to be doing more to mitigate robocalls, such as weak robocall mitigation programs (RMPs), RMPs that are only adhered to inconsistently (including KYUP requirements), or providers who do respond to tracebacks but still continue to carry some illegal

[53] *See, e.g.*, Seventh Report and Order in CG 17-59 (2023), *supra* note 12 at ¶ 30.

traffic.[54] These can also include downstream providers who do not take adequate steps to know their upstream provider[55]—as USTelecom has noted:

> [A] provider identified in tracebacks as accepting significant volumes of illegal traffic from one or more providers with late and/or suspiciously recent entries to the RMD may be indicative of substandard due diligence efforts. Downstream providers that accept traffic from [Robocall Mitigation Database] filers that submit incomplete or incomprehensible robocall mitigation plans, or that include

[54] Several targets of enforcement actions for transmitting illegal robocalls were reported as responding to the majority of traceback requests they received. This underscores the fact that although failure to comply with traceback requests should be grounds for treating an RMD entry as facially deficient, timely compliance with traceback requests is not sufficient to determine whether or not the provider is a good actor. For example, "TCA VOIP / Telecom Carrier Access / TeleSpan", RSCom LTD, Hello Hello Miami, and Mobi Telecom have each been subject to Commission enforcement actions and evidenced high volumes of traceback requests, but all responded to the vast majority of traceback requests they received, per the Commission's four annual reports to Congress. Not one of these providers were listed as non-responsive providers in any year's individual report (a "non-responsive" provider fails to respond to three or more traceback requests in that year). Moreover, even while all four did appear in the Commission's "Non-Responsive ALL TIME" tabs in its 2022 and 2023 reports, each responded to the vast majority of the traceback requests it received. *See* 2023 FCC Report to Congress; 2022 FCC Report to Congress. TCA Voip was subject to actions by both the Vermont Attorney General, *see* Vermont AG Complaint *supra* note 46, and the Commission, *see* (k)(4) cease and desist letter to Dominic Bohnett (Feb. 10, 2022), https://docs.fcc.gov/public/attachments/DOC-380157A1.pdf, but is listed under the "Non-Responsive ALL TIME" tab of the Commission's 2023 report as failing to respond to 4 of the 182 traceback requests it received, *see* 2023 FCC Report to Congress. Similarly, RSCom, *see* (k)(4) cease and desist letter to Vitaly Potapov (Mar. 17, 2021), https://docs.fcc.gov/public/attachments/DOC-370915A1.pdf, also target of Federal Trade Commission (FTC) action, *see* Warning Letter to RSCom Ltd. (May 10, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/pointofnoentry-rscomwarningletter.pdf, is listed under the "Non-Responsive ALL TIME" tab of the Commission's 2023 report as failing to respond to only 8 of the 859 tracebacks it received, *see* 2023 FCC Report to Congress. Hello Hello Miami was subject to Commission action, *see* (k)(4) cease and desist letter to Luis E. Leon (Mar. 22, 2022), https://docs.fcc.gov/public/attachments/DOC-381500A1.pdf, and FTC action, *see* FTC, Law Enforcers Nationwide Announce Enforcement Sweep to Stem the Tide of Illegal Telemarketing Calls to U.S. Consumers (July 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-law-enforcers-nationwide-announce-enforcement-sweep-stem-tide-illegal-telemarketing-calls-us, but is listed under the "Non-Responsive ALL TIME" tab of the Commission's 2023 report as failing to respond to 5 of the 136 traceback requests it received, *see* 2023 FCC Report to Congress. Mobi Telecom was subject to Commission action, *see* (k)(4) cease and desist letter to Davinder Singh (July 7, 2022), https://docs.fcc.gov/public/attachments/DOC-385012A1.pdf, and continuing action in August 2023, *see* FCC Assesses Nearly $300M Forfeiture for Unlawful Robocalls (Aug. 3, 2023), https://www.fcc.gov/document/fcc-assesses-nearly-300m-forfeiture-unlawful-robocalls, but is listed under the "Non-Responsive ALL TIME" tab of the Commission's 2022 report as failing to respond to 5 of the 171 traceback requests received, *see* 2022 FCC Report to Congress. Identical figures are reported for Mobi in the "Non-Responsive ALL TIME" tab of the Commission's 2023 report, *see* 2023 FCC Report to Congress.

[55] Seventh Report and Order in CG 17-59 (2023), *supra* note 12 at ¶¶ 49-50 ("We find that, while intermediate providers may be unable to identify the calling customer with sufficient accuracy to know whether they are placing illegal calls, the Commission cannot permit them to "intentionally or negligently ignore red flags from their upstream providers.").

> inconsistencies or other questionable information in their . . . filings, may too be indicative of a problem worthy of Commission scrutiny.[56]

These efforts can include measures by which to evaluate a RMP that is not just a blank sheet of paper.[57]

While these behaviors are less obvious to detect and may require a more intensive adjudicatory process to correct than facially deficient RMD entries, they are still worthy of the Commission's attention and enforcement.

VIII. Conclusion

We appreciate the Commission's attention to effective improvements to the RMD. We would be happy to answer any questions.

Respectfully submitted, this the 15th day of October 2024, by:

Chris Frascella
Matt Contursi
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036

Peter Gregory
Public Knowledge
1818 N St, NW, Suite 410
Washington, D.C. 20036

Eden Iscil
National Consumers League
1701 K St, NW, Suite 1200
Washington, D.C. 20006

[56] Sixth Report and Order in WC 17-97 (2023), *supra* note 17 at ¶ 38 fn. 147 (citing to USTelecom Reply, CG Docket No. 17-59, WC Docket No. 17-97, at 3, 14 (rec. Sept. 16, 2022)).

[57] *See* Evaluating Robocall Mitigation Programs, Legal Calls Only, https://legalcallsonly.org/mitigation/ (last accessed Aug. 17, 2022). We do not necessarily endorse this methodology, but merely note that factors exist by which a RMP filed in the RMD might be evaluated and found to be deficient.