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 FIFTH FURTHER NOTICE OF PROPOSED RULEMAKING IN WC DOCKET NO. 17-97

by

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

Submitted August 17, 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

While the Commission has undertaken several efforts to mitigate scam robocalls over the last twenty years, in particular since the TRACED Act, the number of illegal robocalls, as well as estimated consumer losses from these calls, continues to grow. We urge the Commission to change the incentive structures that encourage providers to facilitate illegal call traffic and take aggressive action to eliminate these dangerous calls.

Specifically, if it is to effectively eradicate illegal calls, we recommend that the Commission:

1. Require telecommunications providers to achieve effective mitigation outcomes (not merely to take reasonable steps), and hold providers strictly liable for any robocall-related misuse of numbering resources that they facilitate by providing access to those numbering resources.

2. Automatically and quickly suspend high-risk providers from the robocall mitigation database (RMD) if they receive a third traceback request within twelve months; and automatically and quickly suspend any provider who does not adequately respond to traceback requests, who is non-compliant with paying fines or forfeitures, whose management is affiliated with known offenders, or who otherwise evades or fail to comply with Commission rules or orders.

3. Impose licensing and bonding requirements on non-facilities-based providers, so that the Commission can a) easily collect forfeitures and fines from bad actors, and b) effectively exclude known bad actors.

4. Make traceback information public, so more stakeholders can more easily leverage their market power and enforcement authority to combat this persistent scourge.

Table of Contents

Comments

I. Introduction – Scope of the Problem

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 to encourage the Commission to provide incentives and clear mechanisms for all voice service providers to stop transmitting scam calls and illegal robocalls.

In this NPRM,[3] the Federal Communications Commission (FCC, or "Commission") seeks comment on an extensive list of ideas for a proposed rule to protect consumers from illegal robocalls. The proposals under consideration include applying robocall mitigation requirements to all domestic providers in the call path, requiring downstream providers to block calls from non-compliant upstream

[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), the Federal Trade Commission, the federal courts, and state legislatures. 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] *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, 87 FR 42670 (July 18, 2022), available at https://www.federalregister.gov/documents/2022/07/18/2022-13878/advanced-methods-to-target-and-eliminate-unlawful-robocalls-call-authentication-trust-anchor [hereinafter "NPRM"].

providers, limitations on indirect access to U.S. North American Numbering Plan (NANP) numbers, and enhancements to enforcement.[4]

This dockets included in this NPRM[5] address Commission requirements for gateway providers to submit traffic mitigation plans to the Robocall Mitigation Database, apply caller ID authentication to unauthenticated foreign-originated calls using U.S. telephone numbers, respond to traceback requests within 24 hours, block calls that are clearly illegal traffic, and implement "know your upstream provider" obligations, among other requirements.[6] The mandates imposed by these orders on gateway providers, as well as the proposals under consideration in this NPRM, all represent important steps forward in the ongoing battle to stop illegal robocalls. They follow other efforts by the Commission to combat the robocall scourge, including, most recently, reducing the extension of time for providers to comply with STIR/SHAKEN (which took effect on June 30, 2022),[7] ordering blocking of bad actor providers,[8] warning consumers about the rising threat of scam robotexts,[9] and implementing new regulations for gateway providers (to take effect on September 16, 2022).[10]

---

[4] *See id.*

[5] *In re* 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 (May 20, 2022), available at https://docs.fcc.gov/public/attachments/FCC-22-37A1.pdf [hereinafter "Sixth Report and Order"].

[6] *See id.* at ¶ 2.

[7] *See* Fed. Commc'ns Comm'n, FCC Closes Robocall Loophole (June 30, 2022), https://www.fcc.gov/document/fcc-closes-robocall-loophole.

[8] *See* Fed. Commc'ns Comm'n, FCC Orders Blocking of Auto Warranty Robocall Scam Campaign (July 21, 2022), https://www.fcc.gov/document/fcc-orders-blocking-auto-warranty-robocall-scam-campaign [hereinafter "FCC Sumco Order"].

[9] *See* Fed. Commc'ns Comm'n, FCC Warns Consumers of Rising Threat of Scam Robotexts (July 28, 2022), https://www.fcc.gov/document/fcc-warns-consumers-rising-threat-scam-robotexts.

[10] *In re* Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Final Rule, CG Docket No. 17–59, WC Docket No. 17–97, 87 FR 42916 (July 18, 2022), https://www.federalregister.gov/documents/2022/07/18/2022-13436/advanced-methods-to-target-and-eliminate-unlawful-robocalls-call-authentication-trust-anchor.

In the comments filed today, we urge the Commission take this battle up a notch: to issue regulations that are not only more aggressive, but also that impose more comprehensive requirements on providers. The Commission's top priority in this proceeding should be to stop criminals seeking to defraud telephone subscribers through scam calls and the complicit and complacent providers who transmit those calls. We encourage the Commission to address the illegal robocall problem with clear mandates, the violation of which will trigger expedited responses punishing the transgressors. Deterrence is based on the principle that swift, certain punishment prevents misconduct.[11] Just as the law requires the immediate arrest and suspension of a person's driver's license if they are suspected of driving while impaired,[12] the FCC's rules should similarly require immediate action against providers to protect telephone subscribers from illegal calls.

The key to a successful change in the robocall landscape is to provide strong incentives for all providers in the call path to ensure that they are not transmitting illegal calls. The FCC recognizes that America suffers from a persistent problem with robocalls,[13] and its proposed changes in this proceeding will represent a helpful measure of progress, especially if it imposes strict liability for misuse of access to numbering resources and implements policies that prevent bad actors from re-listing themselves

---

[11] *See* National Institute of Justice, Five Things About Deterrence (June 5, 2016), https://nij.ojp.gov/topics/articles/five-things-about-deterrence ("The certainty of being caught is a vastly more powerful deterrent than the punishment.").

[12] License Suspension or Revocation After DUI Convictions, Justia, https://www.justia.com/criminal/drunk-driving-dui-dwi/dui-penalties/license-suspension-revocation/ (last accessed Aug. 17, 2022).

[13] *See* Fed. Commc'ns Comm'n, Stop Unwanted Robocalls and Texts, *available at* https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts ("Unwanted calls—including illegal and spoofed robocalls—are the FCC's top consumer complaint and our top consumer protection priority.") (last accessed Aug. 17, 2022); Statement of Comm'r Geoffrey Starks, (May 19, 2022), https://docs.fcc.gov/public/attachments/FCC-22-37A3.pdf ("Robocalls continue to be the biggest source of complaints the Commission receives."); FCC, Declaratory Ruling and Order, Re: Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, WC Docket No. 07-135 (Jul. 10, 2015) at ¶ 5 , https://www.fcc.gov/ecfs/file/download/60001114787.pdf?file_name=FCC-15-72A1.pdf ("Despite the Commission's efforts to protect consumers without inhibiting legitimate business communications, TCPA complaints as a whole are the largest category of informal complaints we receive."); see also Quarterly Reports – Consumer Inquiries and Complaints, FCC, https://www.fcc.gov/general/quarterly-reports-consumer-inquiries-and-complaints (last accessed Aug. 17, 2022) (dating back to January-March 2002).

under a different name on the Robocall Mitigation Database (RMD). However, neither the new rules, nor even the proposals in the NPRM, will address the root problem: it will still be more profitable to transmit illegal robocalls than to effectively mitigate them.[14] Even if all the proposals are adopted, the consequences for providers transmitting illegal calls are still unclear, depend on specific findings and non-automatic actions by the FCC, and provide limited, delayed—and likely not always effective—protections against providers who are gaming the system and making money by transmitting illegal calls into the U.S. telephone system.

The Magnitude of the Problem. In 2020, the Commission said that scam calls cost the American telephone system $13.5 billion, breaking it out as $3 billion in nuisance and wasted time,[15] and $10.5 billion in lost money.[16] However, direct consumer losses from these illegal calls have ballooned since that initial estimate. In May 2022, TrueCaller, the entity whose survey data the FCC cited to in 2020, released its estimate of nearly $40 billion in consumer monetary losses over the previous twelve months.[17] As with the FCC's 2020 estimate, this updated estimate does not include nonquantifiable harms such as less reliable access to emergency healthcare communications and (continued and further) diminished trust in the U.S. telephone network caused by illegal robocalls.[18]

---

[14] *See* NCLC and EPIC, Scam Robocalls: Telecom Providers Profit (June 2022), available at: https://www.nclc.org/issues/energy-utilities-a-communications/scam-robocalls-will-continue-until-telecom-providers-no-longer-profit-from-them.html [hereinafter "Scam Robocalls Report"].

[15] *See* First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3263, ¶ 47 (Mar. 31, 2020) (10 cents per call, 30 billion scam calls per year).

[16] *See id.* at ¶ 48 ($10.5 billion per TrueCaller 2019 Survey data).

[17] *See* TrueCaller, 2022 U.S. Spam & Scam Report (May 24, 2022), https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report (estimating $39.5 billion in consumer losses over the last twelve months, noting that "[t]he total money lost to scams is also comparable to the entire child care budget of $39 billion for the American Rescue Plan Act. If phone scam fraud was somehow eliminated, the amount saved could fund federally subsidized child care across the U.S. for a full year to help families and employers."). The same source reported $29.8 billion in actual consumer losses in 2021 and $19.7 billion in losses in 2020, an increase of nearly $10 billion every year since 2019. *See id.* at "Total Money Lost to Scam Calls" chart.

[18] *See* Sixth Report and Order at n. 6 (citing to First Caller ID Authentication Report and Order and FNPRM, Call Authentication Trust Anchor, Implementation of the TRACED Act Section 6(a) Knowledge of Customers

Swift Action is Required. As we note in our recent report, more than a billion scam robocalls are made to American telephones every month seeking to defraud American telephone subscribers.[19] This is more than 33 million illegal robocalls every day. Indeed, a single bad actor, aided by the complicit and complacent providers who profit from this trafficking, can be responsible for more than 425 million robocalls in a single 30-day period.[20] Seniors, immigrants, people with disabilities, student loan borrowers, and all American telephone subscribers deserve relief from the robocall scourge now.[21]

Our Proposals. We urge the Commission to simplify its rules and require that the focus be on the results of the provider's efforts to mitigate illegal calls. The regulatory scheme governing providers' mitigation efforts should be easy for all providers to understand and should contain built-in incentives for compliance. Ensuring compliance should not be dependent on individual Commission cease and desist letters, state Attorney General enforcement actions, or FTC enforcement actions. As is clear from the ongoing scourge of a billion-plus illegal robocalls each month,[22] there are too many providers, too many callers, and too many illegal campaigns for that methodology to work.

Instead, we urge the Commission to implement a regulatory structure that allows legitimate callers to leverage marketplace dynamics to incentivize compliance. For example, if legitimate callers can access traceback records, they can see which originating and intermediate providers are responsible

---

by Entities with Access to Numbering Resources, WC Docket Nos. 17-97, 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3263, ¶ 47-48 (2020)) (noting additional intangible costs).

[19] *See* Scam Robocalls Report at 6.

[20] *See* Press Release, The Department of Justice Files Actions to Stop Telecom Carriers Who Facilitated Hundreds of Millions of Fraudulent Robocalls to American Consumers, U.S. Dep't of Justice (Jan. 28, 2020), https://www.justice.gov/opa/pr/department-justice-files-actions-stop-telecom-carriers-who-facilitated-hundreds-millions ("For example, the complaint against the owners/operators of Ecommerce National d/b/a TollFreeDeals.com alleges that the defendants carried 720 million calls during a sample 23-day period, and that more than 425 million of those calls lasted less than one second, indicating that they were robocalls."); United States v. Palumbo, 448 F. Supp. 3d 257, 264 (E.D.N.Y. 2020) (scam calls costing consumers hundreds of thousands of dollars); *id.* at 262 (defrauding an 84-year old consumer of $9,800 by impersonating the U.S. Marshals Service).

[21] *See* Scam Robocalls Report at 7 (links to audio from scam robocall campaigns targeted at vulnerable groups).

[22] *See id.* at 6.

for transmitting the scam calls. They can then avoid hiring those originating providers and require their providers to avoid transmitting their legitimate calls through intermediate providers found responsible for transmitting illegal calls.

We believe that implementing the following four key changes will create the significant change in the regulatory structure needed to protect American telephone subscribers from scam robocalls:[23]

1. The Commission should require all providers to engage in effective mitigation and apply clear, enforceable financial consequences on providers who knew or should have known that they were transmitting illegal robocalls.[24] Effective mitigation should be measured based on results, not on the individual descriptions of the steps promised by providers.

2. The Commission should, after notice, automatically and quickly suspend providers who continue to transmit illegal robocalls from the Robocall Mitigation Database (RMD). This automatic response would signal the Commission's prioritization of the protection of phone subscribers over providers' income streams. This type of action would provide the "swift and certain" punishment that is most effective in deterring repeat offenders.

3. The Commission should impose, or seek Congressional permission to impose, strict licensing and bonding requirements—to ensure that the Commission can easily and quickly collect the forfeitures it has assessed, and to prevent bad actors from re-listing themselves in the RMD.

4. The Commission should require traceback information regarding the top of the call path to be made public, thereby enabling all providers in the call path to see which providers have been responsible for transmitting illegal calls in the past. This will allow providers to avoid either accepting calls from or sending calls to those providers. Public tracebacks would enable a market-based methodology for providers to enforce the rules. This would also enable legal robocallers to ensure that their calls are not routed through providers with a history of tracebacks, thereby protecting those calls from blocking or mislabeling.

---

[23] Earlier versions of these proposals are discussed in further detail in our recent report. *See* Scam Robocalls Report at 26.

[24] Some states have already made great strides here. See, e.g., Complaint for Permanent Injunction, Damages, and Other Equitable Relief, *State of Ohio v. Jones, et al.*, Case No. 2:22-cv-2700 (S.D. Oh. July 7, 2022) [hereinafter "Ohio Complaint"]; Complaint, State of Vermont v. Bohnett, Case No. 5:22-cv-00069 (D. Vt. Mar. 18, 2022) [hereinafter "Vermont Complaint"]; Complaint for Injunctive Relief and Civil Penalties, North Carolina *ex rel.* Stein v. Articul8, LLC & Paul K. Talbot, Case No. 1:22-cv-00058 (M.D.N.C. Jan. 25, 2022) [hereinafter "North Carolina Complaint"]; 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, 2021 WL 4803899 (S.D. Ind. Oct. 14, 2021) [hereinafter "Indiana Complaint"].

Our comments in response to the proposals, ideas, and questions posed by the Commission to deal with illegal scam calls in the NPRM are provided in the context of these four points.[25]

II. Require Effective Mitigation, with Financial Incentives.

The Commission is uniquely positioned to require proactive, immediate, effective mitigation. Doing so should include establishing an "affirmative, effective" standard and imposing strict liability on providers who provide access to numbering resources that are misused to facilitate illegal robocalls.[26] We encourage the Commission to build on its recent, aggressive actions to stop auto warranty scammers by shutting down the providers who transmitted their illegal calls,[27] in conjunction with the Ohio Attorney General's impressive investigation and complaint.[28] In the past, the Commission's cease and desist letters[29] had merely warned that downstream providers would be authorized to block traffic *if the bad actor did not change its practices*. The Commission's announcement in relation to the auto warranty calls represents the first time the Commission has publicly specified a bad actor and ordered

---

[25] *See* Scam Robocalls Report, Appendix 1, for an explanation of the robocalls that are illegal but not scam calls, such as unconsented-to prerecorded calls to cell phones and telemarketing calls to residential lines registered on the Do Not Call Registry without prior express consent. The remedies recommended in these comments are only intended to address blatantly illegal, fraudulent calls.

[26] State AGs have made recent progress on the enforcement front, *see supra* note 24, and moreover seem poised to continue to do so in the near future with the formation of their Anti-Robocall Litigation Taskforce, which has already sent out 20 civil investigative demands (CIDs), *see, e.g.*, Press Release, Attorney General Josh Stein Leads New Nationwide Anti-Robocall Litigation Task Force (Aug. 2, 2022), https://ncdoj.gov/attorney-general-josh-stein-leads-new-nationwide-anti-robocall-litigation-task-force/. However, only the Commission can establish a national standard that governs the entire national telecommunications system.

[27] *See* FCC Sumco Order, *supra* note 8.

[28] *See* Press Release, Yost Files Suit Alleging Massive Robocall Scheme – FCC Joins Fight in Related Action (July 7, 2022), https://www.ohioattorneygeneral.gov/Media/News-Releases/July-2022/Yost-Files-Suit-Alleging-Massive-Robocall-Scheme-F.

[29] *See* Fed. Commc'ns Comm'n, Robocall Facilitators Must Cease and Desist, https://www.fcc.gov/robocall-facilitators-must-cease-and-desist [hereinafter "FCC Cease and Desist Letters"]. Notably ThinQ, recipient of a cease and desist in March 2022, had already received a letter implying non-compliance two years earlier. *See* Enforcement Bureau Requests ThinQ Support in Robocall Traceback (Feb. 4, 2020), https://www.fcc.gov/document/enforcement-bureau-requests-thinq-support-robocall-traceback (last visited August 10, 2022) ("Tracebacks by the USTelecom Industry Traceback Group and the Commission have found that ThinQ is being used as a gateway into the United States for many apparently illegal robocalls that originate overseas.").

downstream providers to block traffic from it immediately. This is a significant and important milestone, and an approach that we encourage the Commission to implement automatically once problematic providers have been warned that they are transmitting illegal calls through the ITG traceback process, other Commission actions, or enforcement efforts by partner agencies.

Investigations and prosecutions of past wrongdoing take months and hundreds of hours to gather, sift and present evidence. Yet in every month, over a billion more illegal scam robocalls assault the telephones and invade the privacy of American subscribers, and thousands of individuals are scammed out of their rent money, or worse. To stop the scam calls, the system protecting subscribers from these assaults needs to be sped up, and measures limiting access through complicit providers must be applied quickly after the provider has been found to have transmitted illegal calls.

a. Establish an "Affirmative, Effective" Standard for Robocall Mitigation.

i. The Commission should not focus on the methodologies providers use, just on the results.

The Commission asks: "*If the Commission should maintain its flexible approach [regarding the requirement to take affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls], is there value in providing further guidance as to how providers can best comply? If so, what might this guidance include? Should the Commission extend a similar requirement to all providers in the call path, in place of or in addition to its existing requirement.*"[30]

We answer that the Commission should maintain a flexible approach regarding exactly which measures are required to be employed by providers. Potential methodologies that are useful should be recommended to providers.[31] But the Commission should not require any particular methodology over

[30] NPRM at ¶ 28.

[31] We have offered examples of possible methodologies the Commission might recommend. *See* Comments of EPIC and NCLC, *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 No. 13-97; WC Docket No. 07-243; WC Docket No. 20-67 (October 14, 2021), https://www.fcc.gov/ecfs/search/search-filings/filing/10153018018985 (Section II listing data-points that could serve as indicators, Section III listing categories of data that providers could monitor to detect those indicators).

another. Instead, the Commission should emphasize that providers are responsible for employing whatever measures are necessary for them to avoid transmitting illegal calls.[32]

The standard for compliance should be based on the success of the effort, not the measures taken. This is particularly important because just as one measure may prove successful one month, scam callers are likely to quickly adopt new methods for evading that successful measure. Providers need to be incentivized to be constantly on the lookout for illegal traffic in the calls they are transmitting.

To eradicate scam robocalls, the Commission must require that providers *effectively* mitigate scam robocall traffic.[33] Compliance should not be evaluated based on what measures the provider says it is using, or even whether it is using the measures promised. Compliance should be evaluated based on the success of the provider's efforts in avoiding the transmission of illegal robocalls.

In the current system, American phone subscribers suffer month after month in large part because providers are permitted to wait until receiving notice from the Commission to block illegal calls,[34] and are merely expected to document in the Robocall Mitigation Database (RMD) the "reasonable steps" they commit to taking to mitigate robocalls. These RMD-documented policies are not evaluated as to whether those efforts are actually effective.[35] Moreover, there is no public record suggesting that the Commission or anyone else with enforcement authority evaluates whether these

---

[32] *See* Sixth Report and Order, at ¶ 92 (declining to define "reasonable analytics" because it could give a road map to bad actors, and as such also declining to require analytics-based blocking, and opting instead for a system that encourages providers to respond to evolving threats).

[33] At present, the Commission has proposed making all providers subject to the requirement to respond to traceback requests and notices from the Commission, § 64.1200(n)(1)-(2), but has not proposed to require all providers to take affirmative, effective measures to prevent customers from using their network to originate illegal calls, § 64.1200(n)(3). *See* NPRM at ¶ 19.

[34] 47 C.F.R. § 64.1200(n)(2). *See* NPRM at ¶¶ 26, 32 (requirements that only trigger upon notification from the Commission).

[35] This is by design, as the current standard is "reasonable" not "effective."

promised commitments have been met.[36] There are questions about the quality of submissions to the RMD,[37] but because the Commission cannot reasonably evaluate the thousands of submissions it has received, there is no practical enforcement mechanism for providers whose plans are not reasonable or whose plans are reasonable but not adhered to.

In short, there are several shortcomings to the Commission's current "reasonable steps" standard. An "affirmative, effective" standard would better reflect the Commission's commitment to prioritizing the protection of phone subscribers over the telecom providers who profit from transmitting scam robocalls. We urge the Commission to hold providers to an "affirmative, effective measures" standard, rather than a "reasonable steps" standard.[38]

ii. Until the Commission implements strict liability, the rules should clearly state that each provider in the call path of a fraudulent call is liable for the consequences of that call if that provider knew or should have known that the call was illegal.

The Commission asks "*If a customer nonetheless uses an originating provider's network to place illegal calls, should we adopt a strict liability standard, or allow the provider to terminate or otherwise modify its relationship with the customer and prevent future illegal traffic*?"[39]

To establish the necessary incentives for self-enforcement of mitigation policies, all providers—not merely originating providers—should be held strictly liable. By holding all providers liable for the illegal calls they process, the ecosystem will be forced to develop enhanced—and more effective—

---

[36] For example, if a provider's Robocall Mitigation Plan (RMP) states that the provider will use behavioral analytics to monitor traffic and follow up with upstream providers whose call traffic meets certain criteria (e.g. high call volume, short call duration, low ratio of unique phone numbers to calls made), there is no public indication that the Commission has a system for evaluating whether the provider is in fact following up with these upstream providers, or documenting exceptional circumstances that justify not following up.

[37] *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.

[38] The Commission asks whether VoIP providers should have a higher burden to meet its "reasonable steps" standard, *see* NPRM at ¶ 37, but we respond that the Commission should apply an "affirmative, effective measures" standard to all providers, including VoIP providers.

[39] NPRM at ¶ 29.

methods to identify and block the illegal calls. That potential liability will create the financial incentives for providers to rapidly adapt to the evolving tactics of bad actors. This flexibility will be more effective than prescriptive requirements.

By way of analogy, the Fair Credit Billing Act (FCBA),[40] which governs the relationship between banks and consumers who use credit cards, illustrates why placing the financial liability on providers for illegal calls will be an effective mechanism to stop scam robocalls. The FCBA imposes the cost of losses from credit card fraud and error on the banks, rather than consumers. As a result, the banking industry has developed a robust set of protections governing the use of credit cards to minimize their own losses from theft, fraud and even user negligence. The banks control the system, imposing on merchants their requirements to protect against losses. While there are extensive regulations issued by federal regulators that govern the transactions between the banks and their customers (*e.g.*, disclosures and rules governing imposition of finance charges), there are no rules governing *how* the banks should protect themselves from losses caused by fraudsters. The banks—which will bear the burden of failure—have every incentive to develop vigorous procedures to limit these losses. The security procedures used by banks to monitor and avoid losses are constantly changing to combat new threats. The Commission can similarly incentivize telephone service providers to develop and use procedures to guard against transmitting fraud robocalls.

Because it will take time for providers to adapt to a strict liability model, in the interim the Commission should implement a "know or should have known" standard to govern provider liability for illegal call traffic.

The Commission should explicitly state that when a provider receives notification from the Industry Traceback Group (ITG), the Commission, or any law enforcement entity that illegal traffic

[40] 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.

may be passing through its network, then the provider is considered to "know" it is transmitting illegal calls. The Commission should also be explicit that when a provider fails to mitigate illegal traffic that the provider itself has detected, it "should have known" it was transmitting illegal calls. Critically, the Commission should make clear that, where providers have a responsibility to take reasonable steps to detect and mitigate illegal call traffic,[41] they cannot evade the "should have known" component of the standard by failing to monitor call traffic.[42]

Even if a provider never receives a traceback request, if its robocall mitigation plan truly consists of "reasonable steps," those steps should include call analytics and possibly also content analytics to identify and stop illegal calls in their tracks.[43] For example, the Social Security Administration (SSA) has been able to achieve a drastic reduction in Social Security scam calls by hiring a vendor to pay close attention to the automated call traffic and alert the downstream providers not to accept this illegal traffic.[44] This is a hugely successful application of traffic analytics. The Commission should create the incentives for providers to use similarly effective methods throughout the system.

Imposing these requirements will mean that the choices that providers in the call path make about whether to accept calls from upstream providers will be guided not only by the price paid for those calls, but also by the likely consumer harm caused by accepting calls from those upstream providers. The consequences for choosing to facilitate consumer harm that should have been anticipated and prevented should be steep.

---

[41] As the Commission proposes requiring. *See* NPRM at ¶ 19.

[42] *See, e.g.*, Vermont Complaint at 1; *id.* at ¶ 120.

[43] *See* Scam Robocalls Report at 16-18; NPRM at ¶ 36.

[44] Private email from Mike Rudolph, CTO, YouMail (July 26, 2022) (showing weekly estimates of imposter scam calls reducing from multiple millions to less than one million).

Legal robocallers will also benefit from this regime, as it will reduce, if not eradicate, the practice of intermediate providers mixing legal calls with illegal calls, thereby reducing mislabeling and incorrect blocking.

Imposing this requirement will not place an unfair burden on downstream providers. They can protect themselves by placing indemnification clauses in their contracts with their upstream providers. Their contracts can provide that the upstream provider will not accept calls from further upstream providers with a history of transmitting illegal calls, a history of failures to respond to tracebacks, or other behaviors that indicate that calls from the provider are likely illegal, and that the upstream provider will indemnify the downstream provider from any losses that result from the upstream provider's transmission of illegal calls to it.

b. Access to Numbering Resources Should Include Strict Liability for Misuse.

The Commission asks *"[i]nstead of or in addition to limiting indirect access, could we hold providers that obtain numbers directly from NANPA strictly liable for illegal robocalling undertaken by any entity that obtains the number through indirect access? Would such an approach be enforceable and, if so, how would we enforce it?"*[45]

We support the Commission's proposal to hold providers strictly liable for illegal robocalling that makes use of numbers the providers rent out. As the Commission notes, there is evidence in the record that unscrupulous providers are providing indirect access to numbering resources for nefarious purposes, including illegal robocalling, and that some illegal robocallers have transitioned from call spoofing to indirectly accessing massive volumes of legitimate numbers for their scam campaigns, thereby bypassing the safeguards of STIR/SHAKEN entirely.[46] Holding providers strictly liable would give them the incentive to diligently investigate a prospective renter of numbering resources before granting use of those numbers. The Commission has authority to hold providers strictly liable for

[45] NPRM at ¶ 68.

[46] *See* NPRM at ¶ 67.

misuse of numbering resources in this way under Section 251(e)[47] and Section 6 of the TRACED Act, through the Numbering Policies for Modern Communication proceeding.[48]

We strongly support the certainty and financial incentives implicated by strict liability, as some providers have already demonstrated their propensity for abuse.[49] We note that it would also be useful, as the Commission has proposed, to track the number of times that a number has been transferred via indirect access, to whom, and who has the right to use a number at a particular time.[50] However, this should be a secondary priority, as it is far more time-consuming and labor-intensive than imposing strict liability on those best positioned to prevent the harm, and consumers need relief immediately. The tracking methodology is likely to be much less effective than strict liability for misuse.

III. Automatically Suspend from the Robocall Mitigation Database (RMD) "High-Risk Providers" that Repeatedly Transmit Illegal Calls and Any Provider that Fails to Comply with Commission Rules or Orders or is Affiliated with a Previously Suspended Provider.

The Commission already has the tools in place to quickly eliminate the transmission of scam robocalls by complicit providers; it just needs to use them. The Robocall Mitigation Database (RMD) is a brilliant method to enforce compliance not only with the implementation of STIR/SHAKEN requirements, but also to enforce compliance with all of the Commission's robocall mitigation

---

[47] Giving the Commission "exclusive jurisdiction over those portions of the North American Numbering Plan that pertain to the United States."

[48] TRACED 6(a)(1) (requiring the Commission to commence a proceeding to determine registration and compliance obligations to ensure voice service providers offering numbering resources "take sufficient steps to know the identity of [their] customers, to help reduce access to numbers by potential perpetrators of violations of section 227(b)"); TRACED 6(a)(2) (giving Commission ability to prescribe regulations that modify policies in a(1) to better achieve goals of a(1)); WC 13-97, Numbering Policies for Modern Communication.

[49] *See, e.g.,* Bandwidth Comment, Numbering Policies for Modern Communications, WC Dkt. No. 13-97, etc. (Nov. 15, 2021) at 10, available at https://www.fcc.gov/ecfs/file/download/Bandwidth%20Numbering%20Reply%20Comments%20(Final%2011-15-21).pdf?folder=11160037820794 (noting that "Piratel's application was approved notwithstanding the lack of detail about its qualifications and the Enforcement Bureau's robocalling warning letter. Piratel went from being granted valuable numbering resources in early summer 2020 to being named in a lawsuit for alleged abuse of those resources in less than a year and a half.").

[50] *See* NPRM at ¶ 68.

requirements on an expedited basis. The threat of de-listing (suspension)[51] is an extraordinarily effective incentive which can be implemented quickly, with immediate consequences for the provider and immediate benefits to protect subscribers from more illegal calls. As of September 28, 2021, de-listing from the Robocall Mitigation Database (RMD) necessarily means that downstream providers are not permitted to accept the call traffic of the deficient provider.[52] However, this surgically precise and effective tool remains unused by the Commission as a way to enforce mitigation requirements.[53]

Because voice service providers make money from connecting calls, whether those calls are legitimate or not, they are currently incentivized to look the other way and accept payment for permitting illegal traffic to reach American phones. That incentive structure needs to change. FCC Commissioner Geoffrey Starks noted this counterproductive dynamic regarding robocalls: "[I]llegal robocalls will continue so long as those initiating and facilitating them can get away with and profit

---

[51] "De-listing" should result in legally effective removal from the RMD, but not actual removal. Rather, suspension should entail a prominent notation that the provider's status is suspended. *See, e.g.*, *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls et al., Comments of ZipDX L.L.C., CG Docket No. 17-59 and WC Docket No. 17-97, at 24 (filed Dec. 7, 2021) ("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.").

[52] 47 CFR § 64.6305(c). The prohibition went into effect on September 28, 2021. *See Wireline Competition Bureau Announces Opening of Robocall Mitigation Database and Provides Filing Instructions and Deadlines*, WC Docket No. 17-97, Public Notice, 36 FCC Rcd 7394 (WCB 2021).

[53] The Commission recently achieved the same result without removing Sumco et al. from the RMD. *See* FCC Sumco Order, *supra* note 8. However, this matter was unusual in that it was associated with arguably the most robust state AG robocall investigation to date. *See* Yost Files Suit Alleging Massive Robocall Scheme, *supra* note 28. This is a step in the right direction for the Commission, as even in the case of John Spiller, it issued a forfeiture rather than imposed mandatory blocking requirements. *See* FCC Fines Telemarketer $225 Million for Spoofed Robocalls (Mar. 18, 2021), https://www.fcc.gov/document/fcc-fines-telemarketer-225-million-spoofed-robocalls. However, consumers are harmed while resources are expended on robust investigations that only target individual providers. This delay and inefficiency are unnecessary, as indicators such as a high-risk provider receiving multiple traceback requests or any provider being non-responsive to traceback requests should trigger automatic suspension from the RMD.

from it. Last year's estimated 46 billion robocalls and last month's estimated 4.1 billion calls are proof positive of that."[54]

The Commission asks: *"Are there any other reasons [beyond deficient certifications, or knowingly or negligently originating illegal robocall campaigns] we should de-list or exclude providers from the Robocall Mitigation Database? …What other provider actions would warrant removal from the Robocall Mitigation Database?"*[55]

It is incumbent on the Commission to stop known bad actors from continuing to operate.[56] To accomplish this, we propose that the Commission establish an expedited procedure that defines a category of "high-risk providers" who are closest to the origination of the illegal robocalls, and provide, consistent with due process, for expedited de-listing (suspension) from the RMD if they continue to facilitate illegal calls even after receiving notice that they were doing so.

We recommend that this expedited suspension process also be applied to any provider that fails to comply with other Commission rules or orders (including non-responsiveness to traceback requests, and failing to pay fines or forfeitures), and any provider who is affiliated with individuals or providers that have been previously subject to Commission action.

---

[54] *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), *available at* https://docs.fcc.gov/public/attachments/FCC-21-105A3.pdf.

[55] NPRM at ¶ 55.

[56] *See* Statement of Comm'r Geoffrey Starks, *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59; Call Authentication Trust Anchor, WC Docket No. 17-97; Report and Order, Order on Reconsideration, Order, and Further Notice of Proposed Rulemaking at 2 (May 19, 2022), https://docs.fcc.gov/public/attachments/FCC-22-37A3.pdf ("If we identify a bad actor, it's time to make it harder to operate. If it's a repeat offender, we should go further.").

We also recommend that the Commission work with its established partnerships with the Industry Traceback Group (ITG),[57] state Attorneys General (AGs),[58] and the Federal Trade Commission (FTC),[59] to consider whether the enforcement efforts pending by those entities might comprise an additional basis to use this expedited suspension process against those providers identified as engaging in transmitting illegal robocalls after notice that they are doing so. When an investigation by an enforcement entity like a state Attorney General's office[60] or the FTC determines that a provider participated in a campaign of in illegal robocalls, the AG or the FTC should notify the provider of the consequences it could face if the Commission's expedited suspension process applies in this situation.

Additionally, downstream providers who discover illegal robocall traffic through their use of mitigation strategies such as call or traffic analytics should be required to notify both the Commission and upstream providers when they determine that upstream providers have been transmitting illegal calls. That notice to the Commission could also trigger the initiation of this process, which would

---

[57] *In re* Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED Act), Report and Order, EB Docket No. 20-22 at ¶ 19 (July 27, 2020), https://docs.fcc.gov/public/attachments/DA-20-785A1.pdf ("The Bureau notes its own experience and finds that the Industry Traceback Group has established an outstanding track record of conducting tracebacks in partnership with the Commission.") ; *In re* Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED Act), Report and Order, EB Docket No. 20-22 at ¶ 15 (August 25, 2021), https://www.fcc.gov/document/fcc-retains-industry-traceback-group-robocall-consortium ("The Traceback Group provided traceback data that supported dozens of federal and state enforcement actions, including Commission investigations.").

[58] *See* Fed. Commc'ns Comm'n, FCC-State Robocall Investigation Partnerships, https://www.fcc.gov/fcc-state-robocall-investigation-partnerships (last accessed Aug. 17, 2022).

[59] *See* Press Release, FCC, FTC Demand Robocall-Enabling Service Providers Cut off Scammers (May 20, 2020), https://www.fcc.gov/document/fcc-ftc-demand-robocall-enabling-service-providers-cut-scammers; Press Release, FTC and FCC Send Joint Letters to Additional VoIP Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls, Fed. Trade Comm'n (May 20, 2020) https://www.ftc.gov/news-events/news/press-releases/2020/05/ftc-fcc-send-joint-letters-additional-voip-providers-warning-against-routing-transmitting-illegal ; FCC-FTC Consumer Protection Memorandum of Understanding, Fed. Trade Comm'n (Nov. 2015) https://www.ftc.gov/legal-library/browse/cooperation-agreements/memorandum-understanding-consumer-protection-between-federal-trade-commission-federal-communications.

[60] For example, the result of any of the 20 CIDs sent by the State AG Anti-Robocall Task Force, *supra* note 26; *See also* Vermont Complaint, Indiana Complaint, North Carolina Complaint, Ohio Complaint, *supra* note 24.

include a notice to the upstream provider that continued determinations will trigger a suspension from the RMD.

Due process issues raised by our proposed expedited process are addressed in subsection (c), *infra.*

a. Automatically Suspend "High-Risk Providers" Whose Services Were Used Repeatedly to Transmit Illegal Calls.

The Commission has identified non-facilities-based VoIP providers as a likely source of a large percentage of scam robocall traffic.[61] As these non-facilities-based VoIP providers typically serve as the originating, gateway, or intermediate providers for the illegal calls, we propose that these VoIP providers be termed "high-risk providers," and that they should be subject to the expedited RMD suspension rules we describe below.

As calls move from the originating or gateway provider[62] to the first intermediate provider, and then down the line to subsequent intermediate providers, they are mixed with calls from other providers. Because some intermediate providers accept both illegal traffic and legal calls, calls from different sources are blended together as traffic passes from provider to provider, making identification of fraudulent calls more difficult the farther a provider is removed from the source of the scam calls.

Our proposal can be viewed as an extension of the Commission's most recent Order requiring gateway providers to "know your customer" and imposing a general mitigation standard on them.[63]

---

[61] *In re* Call Authentication Trust Anchor, Fourth Report and Order, WC Docket No. 17-97, at ¶ 15 (Dec. 10, 2021), https://www.fcc.gov/ecfs/file/download/DOC-5f6d2ce19d000000-X.pdf?file_name=FCC-21-122A1.pdf.

[62] *See* Vermont Complaint at 9 ¶ 37 (D. Vt. Mar. 18, 2022) ("Hence, a fraudulent robocall now most frequently "hops" from a foreign entity to a domestic VSP (as the U.S. point of entry), then on through multiple domestic intermediary domestic VSPs to a large domestic carrier-such as Verizon Wireless or AT&T-that ultimately terminates the call with connection to an actual phone."); *See also* Complaint, United States of America v. Palumbo, Case 1:20-cv-00473, at 10 ¶ 22 (E.D.N.Y. Jan. 28, 2020), available at: https://www.justice.gov/usao-edny/press-release/file/1240536/download ("Tracebacks of many different robocalling fraud schemes have led to the identification of Defendants as a gateway carrier willing to transmit huge volumes of fraudulent robocalls into the country, despite clear indicia of fraud in the call traffic and actual notice of fraud.").

[63] *See* Sixth Report and Order at ¶¶ 96-98, 102.

Intermediate providers, especially those that accept calls directly from bad actor originating or gateway providers, are well-positioned to recognize, and therefore be responsible for, the transmission of illegal calls from upstream providers.[64] These providers should be required to either refuse or block illegal calls coming to them, or suffer the consequences of transmitting them on downstream. Currently, the Commission permits but does not require them to do so.[65]

We propose that only these "high-risk providers" be subject to the expedited suspension procedure from the RMD for continuing to transmit illegal calls after receiving a third traceback request within a 12-month period. The traceback process itself informs each of the voice service providers in the call path, including all the intermediary providers, that a traceback through that provider's system is being conducted, and that the traceback relates to an illegal robocall. As explained in the recent complaints filed by both the North Carolina and Vermont Attorneys General, the ITG provides a notice to each provider in the call path explaining that they have transmitted "suspected and known fraudulent and/or illegal robocalls."[66] The ITG usually includes a link to an audio recording of the illegal robocall along with the notice it sends to each provider.[67] So, even if the providers did not know before they received the traceback request from the ITG that the calls transmitted over their networks were illegal, the providers are fully aware once the traceback requests start arriving.

---

[64] The Commission seems to have observed this as well in its September 2021 Gateway Provider Notice. *See* Sixth Report and Order at ¶ 17-18 (extending mandatory blocking requirements to "gateway providers and the providers immediately downstream in the call path," and citing to Gateway Provider Notice at ¶ 28-29, 38-102); *id.* at ¶ 74, 78.

[65] *In re* Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Final Rule, CG Docket No. 17–59, WC Docket No. 17–97, 87 FR 42916 at ¶ 56 (July 18, 2022), https://www.federalregister.gov/documents/2022/07/18/2022-13436/advanced-methods-to-target-and-eliminate-unlawful-robocalls-call-authentication-trust-anchor ; *In re* Advanced Methods To Target and Eliminate Unlawful Robocalls, 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 at ¶ 56 (Oct. 1, 2021), https://docs.fcc.gov/public/attachments/FCC-21-105A1.pdf.

[66] North Carolina Complaint, *supra* note 24, at 12 ¶ 42. *See also* Vermont Complaint, *supra* note 24, at 14 ¶ 57.

[67] *See* Vermont Complaint, at 13 ¶ 53.

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. Yet often there are multiple traceback requests sent to the same provider, each announcing that the provider is suspected of transmitting illegal calls, and the provider is permitted to continue its business: transmitting these dangerous calls to American telephone subscribers. For example, in the Vermont Attorney General's case against a gateway provider known as TCA VOIP, the defendant had been the recipient of an astonishing 132 tracebacks requests.[68]

Intermediate providers are also complicit if they continue transmitting calls from gateway or originating providers after receiving notices that calls they transmitted from those providers were the subject of multiple traceback requests. For example:

- In a case against gateway provider Startel brought by the Indiana Attorney General, a defendant downstream intermediate provider, Piratel, received four traceback requests in three weeks about calls it accepted from Startel.[69]

- In a case brought against Articul8, another intermediate provider, by the North Carolina Attorney General, the defendant had received 49 traceback requests.[70]

Imposing forfeitures on providers who continue to transmit illegal traffic after being notified by the Commission to block that traffic, as proposed by the Commission, would not be nearly as effective in

---

[68] *See* Vermont Complaint, *supra* note 24, at 17 ¶ 79.

[69] *See* 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).

[70] *See* North Carolina Complaint, *supra* note 24, at 30 ¶ 94.

protecting subscribers from the illegal calls, and certainly not as immediate as an automatic suspension from the RMD.[71] If providers continue transmitting illegal calls from the same upstream providers after receiving multiple traceback requests informing them that calls from that upstream provider are illegal, they have already been clearly informed that their services were being used to break the law and defraud vulnerable Americans.[72] The Commission needs to shut that illegal activity down promptly.

b. Automatically Suspend Providers Who Evade or Fail to Comply with Commission Rules, Including Traceback Requests.

We also encourage the Commission to suspend providers who evade or fail to comply with traceback requests or other Commission rules or orders. This would include providers who do not pay Commission-assessed fines or forfeitures, or whose management is comprised of individuals associated with previous misconduct. This policy should apply to all providers.

First, providers should be suspended automatically if they fail to comply with a traceback request in a timely manner.[73] The traceback process is a key element in establishing an effective policy for eradicating illegal robocalls. If providers can disregard traceback requests without consequences, the Commission's goals will be severely undermined. Penalties that incentivize providers to fully and timely comply with traceback requests will facilitate rapid detection and cessation of illegal call campaigns.

The importance of creating penalties that will increase providers' incentive to comply promptly with trackback requests is demonstrated by the evidence that some providers are not taking even the current traceback requirements seriously. In its 2021 report to Congress, the Commission listed 123

---

[71] *See* NPRM at ¶ 53.

[72] *See* Scam Robocalls Report at 15; Indiana Complaint at ¶ 316, *supra* note 69.

[73] For an example of why timeliness is important, see Ohio Complaint at 20 ¶ 69 ("For example, when a VoIP Provider of Sumco Panama had to respond to an ITG traceback request, Sumco Panama needed to 'buy some time' before responding in order to *add* 'auto services' language to the list of opt-in websites in the terms and conditions *after* many VSC robocalls were made based on the alleged 'opt in' from these websites") (emphasis original); *id.* at 19-20 ¶ 68-71.

providers who did not comply with one or more traceback requests.[74] Of these 123 providers, 62 were also listed in the Commission's 2020 report to Congress as non-compliant with one or more tracebacks.[75] More than 10 of these repeat offenders were U.S.-based providers.[76] Prior to the Commission's recent action in conjunction with the Ohio AG's case against Sumco,[77] the Commission had taken no public action taken against these providers,[78] nor provided any public explanation for why no action had been taken. It is unclear why the Commission would permit a provider to disregard traceback requests with impunity for two or more years. If it is to effectively eradicate illegal calls, the Commission must make it more costly for providers to flout compliance with traceback requests.[79]

The Commission has proposed new robocall mitigation requirements, including an expansion of the obligation to provide information in RMD certifications on all domestic providers.[80] However, rather than simply requiring providers to furnish information on robocall mitigation efforts, compliance should be measured by success in eliminating illegal calls and responsiveness to traceback requests.

Second, we urge the Commission to automatically suspend providers from the RMD who have failed to pay fines or forfeitures to the Commission. Fines and forfeitures are toothless if they are never

---

[74] *See* Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information at Attachment A, "Non-Responsive" tab (Dec. 22, 2021), https://docs.fcc.gov/public/attachments/DOC-378593A1.pdf [hereinafter "FCC 2021 Report to Congress"].

[75] Compare list from note 72 with Fed. Commcn's Comm'n, Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information at Attachment D, "Non-Responsive" tab (Dec. 23, 2020), https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2020-congress [hereinafter "FCC 2020 Report to Congress"].

[76] *Id.,* filtering by Country: United States.

[77] *See* FCC Sumco Order, *supra* note 8.

[78] *See* FCC Cease and Desist Letters, *supra* note 29. None of the 123 providers listed as non-compliant with a traceback request in the Commission's 2021 report to Congress received a cease-and-desist letter in 2020 nor 2021.

[79] More than five providers, at least two of which were U.S.-based, were non-responsive to three or more traceback requests in 2021, after having been non-responsive to three or more traceback requests in 2020. *Compare* FCC 2021 Report to Congress Attachment A, "2021 NR Providers" tab *with* FCC 2020 Report to Congress Attachment D, "2020 NR Providers" tab.

[80] *See, e.g.*, NPRM at ¶ 42, 48.

collected. Although the Commission may have difficulty collecting its forfeiture orders, it can suspend a provider's livelihood until the forfeiture is paid.

A third ground for automatic suspension should be a finding that a provider's management is comprised of individuals who have been subject to Commission action before. For example, John Spiller, along with other individual and corporate defendants, was assessed the largest fine in Commission history in June 2020 for his role in spoofing phone numbers, calling numbers on the Do Not Call registry, and calling wireless phones without first obtaining consumer consent.[81] However, there is reason to believe he is still facilitating illegal robocalls today, under a different business name.[82] Clearly, more needs to be done to ensure that known bad actors are prevented from continuing to poison the telephone ecosystem.

c. Address Due Process Concerns.

Certainly, due process should be ensured before providers are suspended from the RMD. However, for every day that a provider known to be transmitting illegal calls is *not* suspended from the RMD, that provider is able to continue transmitting tens of thousands additional scam robocalls to American subscribers.[83]

We suggest that the due process rights of providers can be protected even as the Commission prioritizes the needs of U.S. telephone subscribers to be free of illegal robocalls by expediting the

---

[81] *See* Press Release, Fed. Commc'ns Comm'n, Health Insurance Telemarketer Faces Record FCC Fine of $225 Million for Spoofed Robocalls (Mar. 17, 2021), https://docs.fcc.gov/public/attachments/DOC-370869A1.pdf.

[82] Biographical information about John Spiller was included on the About Us page of Great Choice Telecom, but this page has since been taken down. However, at the time of this writing, very similar information is provided on the A Road to Christ website. The contact information for these two organizations is identical, including the phone number and the suite number. *Compare* https://web.archive.org/web/20220330212507/https://aroadtochrist.org/about-us/, *with* https://web.archive.org/web/20220228151117/greatchoicetelecom.com/. The Commission sent a cease and desist letter to Great Choice Telecom in early 2022, but did not reference John Spiller. *See* Letter from FCC to Mikel Quinn, CEO of Great Choice Telecom (Feb. 10, 2022), available at: https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-great-choice-telecom.

[83] As we note in our recent report, the top 1,000 scam robocall campaigns alone account for more than 458 million illegal calls monthly, or over 15 million calls daily. *See* Scam Robocalls Report at 31, n 7.

process of suspending providers from the RMD. Here we suggest an outline of ideas on how the due process concerns may be addressed while meeting the public's need to immediately stop providers from continuing their illegal transmission of scam robocalls. Given the preliminary nature of this discussion, rather than providing a comprehensive analysis of the due process issues, we only seek to show that the Commission can establish a legally valid procedure that protects American telephone subscribers from known bad actors much earlier in the process than is currently the case.

Due process issues raise three concerns: 1) the timing and the content of notice given to the provider before the punishment is applied (suspension from the RMD); 2) the opportunity for the provider to be heard and contest the factual basis for the suspension; and 3) the extent of the punishment to be applied.[84]

The Commission can establish an expedited process of suspending providers from the RMD for any one of the triggering activities akin to that established for a court to provide a Temporary Restraining Order (TRO) pursuant to Rule 65(b) of the Federal Rules of Civil Procedure. TROs recognize the need to move quickly and without prior notice to the respondent to protect the moving party from immediate, irreparable harm.[85]

The Supreme Court has noted that "(D)ue process is flexible and calls for such procedural protections as the particular situation demands."[86] In this context, the Commission will be protecting telephone subscribers from the tens of thousands of illegal robocalls that would otherwise be placed but for the provider's suspension from the RMD. Protecting American subscribers from access by

---

[84] *See, e.g.,* Mathews v. Eldridge, 96 S. Ct. 893, 901 (1976) ("Procedural due process imposes constraints on governmental decisions which deprive individuals of 'liberty' or 'property' interests within the meaning of the Due Process Clause of the Fifth or Fourteenth Amendment.").

[85] "Temporary restraining order", Legal Information Institute, https://www.law.cornell.edu/wex/temporary_restraining_order (last accessed Aug. 17, 2022).

[86] Mathews v. Eldridge, 96 S. Ct. 893, 909 ("In assessing what process is due in this case, substantial weight must be given to the good-faith judgments of the individuals charged by Congress with the administration of social welfare programs that the procedures they have provided assure fair consideration of the entitlement claims of individuals.").

known criminals who seek to defraud them is preventing irreparable harm. Preventing irreparable harm justifies a truncated procedure that provides notice to the provider of the suspension simultaneously with initiating an immediate suspension from the RMD. The Supreme Court has recognized that the Government's interests, as well as the administrative burdens, are to be balanced in these types of situations.[87]

Formal Notice. As when a TRO is issued by a court, the Commission would issue a formal notice of the suspension to the provider at the same time it orders the suspension from the RMD. The notice to the provider would inform it of the basis for the suspension, the provider's right to request an evidentiary hearing to challenge the suspension, and other requirements related to the suspension. At the same time, the Commission should also notify all other providers on the RMD that they are prohibited from accepting calls from the suspended provider, until otherwise notified.

Pre-Suspension Notice. The Commission can ensure that providers subject to these immediate suspensions have received previous notices of the consequences of continuing to transmit illegal calls. Currently, when the ITG sends a traceback request to a provider, it already includes information about the nature of the call subject to the traceback.[88] In the future, the ITG notices to high-risk providers could also include a formal notice from the Commission stating that if the recipient provider receives a third traceback request within a 12-month period it will be suspended from the

---

[87] *Id.* at 902–03 ("Accordingly, resolution of the issue whether the administrative procedures provided here are constitutionally sufficient requires analysis of the governmental and private interests that are affected. . . . More precisely, our prior decisions indicate that identification of the specific dictates of due process generally requires consideration of three distinct factors: First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.") (internal citations omitted).

[88] *See* North Carolina Complaint, *supra* note 66, and Vermont Complaint, *supra* note 66.

RMD.[89] The same would apply to the suspension of providers for failing to comply with traceback requests, or other failure to comply with Commission orders.

Opportunity to be Heard. Once a provider is given the formal notices from the Commission or its enforcement partners about the suspension, the basis for the suspension, and the provider's rights, the provider would have the right to contest the determination that it was transmitting illegal calls, had failed to comply with a traceback request or a Commission order, or was affiliated with providers previously suspended from the RMD.

The Commission should establish a mechanism to allow this type of fact-finding proceeding, possibly before a Commission Administrative Law Judge,[90] on an expedited basis. The Supreme Court has not required that these due process hearings always involve full evidentiary hearings and oral testimony; hearings can be conducted solely through the submission of written evidence.[91] The public's interest (in being relieved of the illegal calls) is a factor in determining the process that that is due. As the Court noted:

> In striking the appropriate due process balance the final factor to be assessed is the public interest. This includes the administrative burden and other societal costs that would be associated with requiring, as a matter of constitutional right, an evidentiary hearing upon demand in all cases prior to the termination of disability benefits. The most visible burden would be the incremental cost resulting from the increased number of hearings . . . .[92]

However, in this context, the Commission's priority should be protecting subscribers from the criminals seeking to defraud them through the scam robocalls. Moreover, the only procedures required are those "to insure that [the respondents] are given a meaningful opportunity to present their case."[93]

---

[89] *See* Section III(a), *supra*.

[90] Administrative Law Judges, Fed. Commc'ns Comm'n, https://www.fcc.gov/administrative-law-judges (last accessed Aug. 17, 2022).

[91] Mathews v. Eldridge, 96 S. Ct. 893, 902, 907-08 (1976).

[92] *Id.* at 909.

[93] *Id.*

And the Supreme Court has emphasized that "substantial weight must be given to the good-faith judgments of the individuals charged by Congress with the administration of social welfare programs that the procedures they have provided assure fair consideration of the entitlement claims of individuals."[94] Like the Social Security Administration in the case quoted, the Commission is charged with the important task of protecting the American public—here, from illegal robocalls.

Length of the Suspension. The Commission should offer the suspended provider the opportunity to request a hearing within an appropriate number of days to contest the grounds for the suspension, provide evidence, and possibly sufficient sureties of good behavior in the future. If no hearing is requested, however, the Commission should determine the appropriate length of the suspension based on the need to protect the telephone system from illegal robocalls.

Permanent suspension from the RMD should be a valued tool in the Commission's authority to protect subscribers from illegal robocalls. This aligns with Commissioner Starks' statement: "[i]f we identify a bad actor, it's time to make it harder to operate. If it's a repeat offender, we should go further."[95] The Commission has already made clear in numerous instances that providers must comply with its rules and has listed potential consequences for failing to do so.[96]

In summary, the proposed suspension procedure should be:

1. The ITG should be required to provide a report to the Commission of each of the following events:

---

[94] *Id.*

[95] *See* Statement of Comm'r Geoffrey Starks (May 19, 2022), *supra* note 56.

[96] For example, since at least as early as its Second Report and Order in October 2020, the Commission has given U.S. voice service providers (as well as foreign providers that use U.S. numbers to send voice traffic to U.S. subscribers) notice that deficient certifications or failure to meet the standards of its own certifications could be met with enforcement "including de-listing the provider from the database." *In re* Call Authentication Trust Anchor, Second Report and Order, WC Docket No. 17-97 at ¶ 93 (Oct. 1, 2020), https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf. Also, that providers must submit updates regarding "any of the information they filed in the certification process" within 10 business days of the change. *Id.* The Commission took a similar step against the robocallers themselves in 2020. *See* Press Release, FCC to Robocallers: There Will Be No More Warnings, Fed. Commc'ns Comm'n (May 1, 2020), https://docs.fcc.gov/public/attachments/DOC-364109A1.pdf.

a. A traceback showing that a provider defined as a "high-risk provider" has transmitted illegal robocalls.

b. A provider who fails to respond to an ITG traceback request.

2. When the Commission receives information from ITG indicating that a high-risk provider has transmitted illegal calls a third time in a 12-month period, or any provider has failed to respond to an ITG traceback request within the required period for response, the Commission should promptly initiate the RMD suspension process:

    a. The provider should be immediately de-listed from the RMD.

    b. The Commission should send the provider a notice outlining the basis for the suspension and explaining what steps the provider can take to request a hearing and the lifting of the suspension, if that is possible in context.

3. If the provider requests a hearing to challenge the basis of the suspension, the Commission should accord the provider the right to an evidentiary proceeding regarding the basis for the suspension, with an appropriate hearing officer. The hearing officer should determine whether the factual basis for the suspension exists and issue a finding accordingly.

The Commission should apply a similar process for notices received from other enforcement partners, such as state AGs or the FTC, and apply a similarly expedited model to suspend from the RMD violators of other Commission orders, such as non-payment of forfeitures and affiliation with a provider who was previously suspended from the RMD.

IV. Impose Licensing and Bonding Requirements to Facilitate Forfeitures and Prevent Offenders from Re-Listing in the RMD.

We are encouraged by the Commission's proposal to prevent offenders who are suspended from the RMD from merely re-listing themselves under another name, as reflected by the Commission's question: *Will such information help identify bad actors and further our enforcement efforts, such as by identifying bad actors previously removed from the Robocall Mitigation Database that continue to be affiliated with other entities filing in the Robocall Mitigation Database?*[97]

While we applaud the Commission's consideration of ways to exclude individuals with a history of complicity with illegal robocalls from the RMD, we are skeptical that the measures identified by the

[97] NPRM at ¶ 46.

Commission[98] will be adequate to catch sophisticated bad actors. The proposed measures are a step in the right direction, but more can be done to prevent bad actors from simply re-listing themselves under a different name.

Typically, the originating or gateway providers that service fraudulent robocallers, and the first few intermediate providers for these calls, are small companies using VoIP (Voice over Internet Protocol) services.[99] Yet, there are currently no meaningful entry requirements for these providers. As a Special Agent with the Social Security Administration's Office of the Inspector General noted:

> In the course of this investigation, I learned that with little more than off-the-shelf VoIP technology, an autodialer, and a business relationship with a gateway carrier, any individual or entity with a broadband internet connection can introduce unlimited numbers of robocalls into the U.S. telephone system from any location in the world.[100]

The VoIP providers that process the illegal robocalls are generally small and have no facilities. They are often one or two individuals with minimal investment or technical expertise who have set up a service in their home or other temporary quarters and offer services through online advertisements.[101] This enables them to nimbly change names and register their business under different names to avoid

---

[98] *See, e.g.*, NPRM at ¶ 52 ("…establish additional bases for removal from the Robocall Mitigation Database, including by establishing a "red light" feature to notify the Commission when a newly-filed certification lists a known bad actor as a principal, parent company, subsidiary, or affiliate; and …subject repeat offenders to proceedings to revoke their section 214 operating authority and to ban offending companies and/or their individual company owners, directors, officers, and principals from future significant association with entities regulated by the Commission."); at ¶ 46 ("we propose to require filers to add information regarding principals, known affiliates, subsidiaries, and parent companies"); at ¶ 56 (considering whether 5% ownership is sufficient to trigger enforcement against "attributable principals").

[99] *See* Appendix to Complaint, United States of America v. Palumbo, Case 1:20-cv-00473, Declaration of Marcy Ralston, at 10 ¶ 20 (E.D.N.Y. Jan. 28, 2020), available at: https://www.justice.gov/usao-edny/press-release/file/1240536/download.

[100] *Id.*

[101] *See id.* at 12-13 ¶ 24 ("Those records further demonstrate that since at least 2016, Nicholas and Natasha Palumbo have operated TollFreeDeals as a VoIP carrier, originally out of their home in Scottsdale, Arizona, and since mid-2019 out of their current home in Paradise Valley, Arizona."); Ryan Tracy & Sarah Krouse, *Where Robocalls Hide: the House Next Door*, The Wall St. J., Aug. 15, 2020, *available at* https://www.wsj.com/articles/where-robocalls-hide-the-house-next-door-11597464021 ("Mr. Palumbo accumulated more than $3.2 million on the hundreds of millions of calls routed through a telecom operation based in his Paradise Valley, Ariz., home last year.").

detection. It also likely contributes to their ability to avoid paying fines and forfeitures imposed by the Commission.[102]

An easy way to create immediate incentives for compliance with the Commission's rules is to require significant bonds for appropriate VoIP providers. Once forfeitures are assessed, the bonds could simply be seized by the Commission as payment. The VoIP businesses with bonds that were seized, and their principals, would likely have significant difficulty obtaining bonds in the future, which would prevent them from regaining access to the U.S. telecommunications system. Bonding is common in high-risk industries such as public construction projects.[103]

We recommend that the Commission require licensing and bonding of all non-facilities-based VoIP providers, but that the bonding requirement be adjusted based on the risk posed by the provider. Specifically, all non-facilities-based VoIP providers should be required to submit applications for a license to operate a VoIP business that transmits calls into the United States. Requirements for bonds should be tailored to the degree of risk associated with the applicant.

For example, applicants who have registered on the RMD previously under the same name, and with the same administrative officers, for the past two years, and for whom there is no known association (through tracebacks or otherwise) with illegal robocalls might be allowed to post a bond of a minimal amount—for example, $10,000.[104] However, applicants that have not previously registered on the RMD, or who have different administrative officers than those previously listed, or for whom there

---

[102] *See* Statement of Chairwoman Jessica Rosenworcel, *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59; Call Authentication Trust Anchor, WC Docket No. 17-97; Report and Order, Order on Reconsideration, Order, and Further Notice of Proposed Rulemaking (May 19, 2022), https://docs.fcc.gov/public/attachments/FCC-22-37A2.pdf ("We also need more tools from Congress to catch those behind these calls, including the ability to go to court directly and collect fines from these bad actors—each and every one of them.").

[103] *See, e.g.,* The Surety and Fidelity Association of America, The Importance of Surety Bonds in Construction (July 2019), https://azdot.gov/sites/default/files/2019/07/Importance_Of_Surety_Bonds_I.pdf.

[104] We address this in Proposal 5 of our recent report in the context of insurance for consumer losses, but there is a significant benefit in deterring bad actors from attempting to re-list themselves as well. *See* Scam Robocalls Report at 30.

is any history of tracebacks, should be required to post bonds of at least $1 million, as tens of millions of Americans are collectively losing billions of dollars to scam robocalls every year.[105]

Bonds would add teeth to the licensing requirements. Bonding and collecting on bonds would also simplify remedies for harm that providers perpetrate or facilitate against consumers. The bond should be applied to unpaid forfeitures, fines, and fees levied by the Commission for non-compliance with its rules, and to compensate defrauded consumers.

If it is to effectively eradicate illegal calls, the Commission must prevent bad actors from evading the financial consequences of their actions and from re-listing themselves in the RMD.

V. Make Tracebacks Public, Including Required Responses, within 24 Hours.

Failing to make traceback information public wastes a valuable resource in the battle to stop illegal calls. We urge the Commission to make traceback information public.[106]

In 2019, through the TRACED Act,[107] Congress mandated that the Commission designate an entity to lead private-sector efforts to trace the origins of illegal calls. For two years, the Industry Traceback Group (ITG) has served this role, delivering data on provider compliance with traceback requests, among other topics, to inform the Commission's reports to Congress in 2020[108] and 2021.[109] However, these reports and other public reporting by the ITG have been inadequate to inform key

---

[105] *Id* at 9. *See* Section I, *supra*.

[106] *See* Scam Robocalls Report at 29-30 ("Proposal 4: All tracebacks conducted by the ITG should be made public."). Improving traceback transparency has been supported by public officials at the federal and the state level. *See, e.g.*, Press Release, Thune, Markey Urge FCC to Continue Fighting Illegal Robocalls, Encourage Increased Transparency Into Trace-Back Efforts (Feb. 4, 2022), https://www.thune.senate.gov/public/index.cfm/2022/2/thune-markey-urge-fcc-to-continue-fighting-illegal-robocalls-encourage-increased-transparency-into-trace-back-efforts; Press Release, Luján Leads Colleagues Urging FCC to Increase Robocall Accountability and Transparency (June 22, 2022), https://www.lujan.senate.gov/newsroom/press-releases/lujan-leads-colleagues-urging-fcc-to-increase-robocall-accountability-and-transparency/; Letter from Bob Ferguson, Attorney General of Washington, to Chair Rosenworcel (July 25, 2022), available at https://twitter.com/agowa/status/1551604985887985664.

[107] Section 13(d).

[108] FCC 2020 Report to Congress, *supra* note 75.

[109] FCC 2021 Report to Congress, *supra* note 74.

stakeholders, such as callers making legal robocalls, downstream providers, state enforcement entities, the victims of the scam calls, and the general public, about which providers are the bad actors exposing American subscribers to the obnoxious, dangerous, and illegal calls.

Currently the ITG keeps the information about traceback findings largely private. This is an irrational squandering of the powerful potential of the traceback process. First, information about completed tracebacks would have enormous value to providers seeking to avoid transmitting scam calls, as it would enable them to identify and avoid accepting calls from the gateway, originating, and intermediate providers that have been found in previous tracebacks to have repeatedly transmitted these calls. Making traceback requests public would also enable scam victims and consumer advocates to identify complicit providers and hold them liable.

Legal robocallers will also significantly benefit from publicly available traceback information. Public traceback information would enable legal robocallers to identify and avoid those originating providers that are transmitting illegal calls. By ensuring that their calls are no longer mixed with the scam calls, the legal robocallers should be able to reduce by a significant degree the extent to which their calls are mislabeled "SCAM CALL" or "SCAM LIKELY." And the number of mistakenly blocked legal calls will also be significantly reduced. Legal robocallers could also require that their originating providers not transmit calls through any intermediate providers that have been repeated recipients of tracebacks.

To accomplish this, the Commission should require that all tracebacks conducted by the ITG be made public within 24 hours of the traceback. This aligns with the Commission's proposed requirement that providers respond to tracebacks within 24 hours,[110] which we support. To ensure the privacy of the subscribers receiving the calls, the last four digits of the subscriber's telephone number in

[110] *See* NPRM at ¶ 22.

each traceback should be redacted. These steps would place market pressure on the originators and the facilitators of scam calls.

If it is to effectively eradicate illegal calls, the Commission must make traceback information public, so more stakeholders can more easily leverage their market power and enforcement authority to combat this needlessly persistent scourge.[111]

VI. Conclusion

We appreciate the opportunity to respond to the Commission's NPRM on eliminating unlawful robocalls.

Respectfully submitted, this the 17th day of August 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

[111] Since March 2018, and possibly earlier, the Commission has referred to illegal robocalls as a scourge. *See* Fighting the Scourge of Illegal Robocalls, Fed. Commc'ns Comm'n and Fed. Trade Comm'n Joint Policy Forum (Mar. 23, 2018), https://www.fcc.gov/fcc-ftc-robocalls-forum.