Testimony before the

SENATE COMMITTEE ON COMMERCE, SCIENCE & TRANSPORTATION

Subcommittee on Communications, Media, and Broadband

Regarding

Protecting Americans from Robocalls

Testimony written and presented by:

Margot Freeman Saunders
Senior Counsel
National Consumer Law Center

On behalf of
the low-income clients of the National Consumer Law Center
and
Consumer Federation of America

October 24, 2023

Margot Saunders
National Consumer Law Center
1001 Connecticut Ave, NW
Washington, D.C. 20036
(202) 452 6252
msaunders@nclc.org
www.nclc.org

Protecting Americans from Robocalls

Chairman Luján, Senator Thune, and Members of the Committee, I appreciate the opportunity to testify today on what needs to be done to protect Americans from robocalls. I provide my testimony here today on behalf of the low-income clients of the **National Consumer Law Center (NCLC)**, and the **Consumer Federation of America**.[1]

The current regulatory structure allows criminals access to Americans' wallets: billions of dollars are stolen every year through scams executed over this nation's telephone lines.[2] At the same time, the combination of the scam calls along with the onslaught of unwanted—and mostly illegal—telemarketing calls and texts damages our trust in our phones and makes it more difficult for important messages from health care providers and other legitimate callers to get through.

The Federal Communications Commission (FCC or Commission) has been trying to address the problems, but, to date, its methods have not succeeded in achieving a meaningful reduction in these unwanted and illegal calls. Either the FCC does not have sufficient legal tools to stop these unwanted and illegal calls, or it has not yet determined how to deploy those tools effectively. In **Section I**, we describe the magnitude of the onslaught of the scam and illegal telemarketing calls, and how the problems caused by these calls have not significantly abated. We note that the numbers of these calls have remained high, despite the dozens of new regulations and rulings issued by the Commission to deploy the STIR-SHAKEN caller-ID authentication technology[3] and implement other mandates of the TRACED Act passed by Congress in 2019,[4] and the enforcement actions it has brought against VoIP providers and illegal callers.[5]

---

[1] This testimony was written with the substantial assistance of Chris Frascella, Counsel at the Electronic Privacy Information Center, and Carolyn Carter, Deputy Director, National Consumer Law Center.

[2] *See* National Consumer Law Center and Electronic Privacy Information Center, *Scam Robocalls: Telecom Providers Profit* (June 1, 2022), *available at* https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/[hereinafter Scam Robocalls report]. This report also explains how scam calls are impacting American subscribers, the mechanics of the communications system in the U.S., how the current system facilitates the transmission of illegal calls, and our recommendations to resolve the problem.

[3] *See* Federal Commc'ns Comm'n, Combating Spoofed Robocalls with Caller ID Authentication, *available at* https://www.fcc.gov/call-authentication.

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

[5] *See In re* Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor, Seventh Report and Order, Eighth Further Notice of Proposed Rulemaking and Third Notice of Inquiry, CG Docket No. 17-59, WC Docket No. 17-97, at ¶¶ 6 to 64. (Rel. May 19, 2023), *available at* https://docs.fcc.gov/public/attachments/FCC-23-37A1.pdf [hereinafter FNPRM].

In **Section II**, we explain that we believe that these scam and illegal telemarketing calls *can* be dramatically reduced. But the resolution requires a shift in emphasis by the FCC. The primary goal of the FCC's actions should be to protect the nation's telephone subscribers from the scam calls that are stealing tens of billions of dollars from them. To do that requires a change from ensuring that calls be completed and protecting voice service providers' access to the telephone network toward shielding consumers from these illegal calls. We believe the number of illegal calls would be significantly reduced if the FCC were to adopt a system of swiftly suspending the ability of complicit providers to transmit illegal calls after they has been notified of previous illegal transmissions.

In **Section III, we** explain our advocacy before the Commission to encourage it to issue guidance that will radically reduce the number of illegal telemarketing calls.

Finally, **Section IV** describes a methodology that would provide legal callers—such as health care providers, callers with fraud alerts, and those with payment reminders—a way to ensure that their calls are completed and that would also facilitate the blocking of the illegal calls.

I. Illegal and unwanted scam and telemarketing calls persist, despite FCC efforts.

The unrelenting onslaught of unwanted and illegal calls and texts to American telephone lines illustrates that more aggressive measures must be employed to stop them. In recent years, the combined number of scam and likely illegal telemarketing calls made every month to American telephone lines has ranged from 1.5 to 3.3 billion every month, with little change from year to year.[6]

While the FCC and the private Industry Traceback Group (ITG)[7] have removed hundreds of offending callers from the network—including progress on scam robocalls regarding car warranties and student loan debt relief[8]— the raw number of illegal calls has remained relatively steady. This

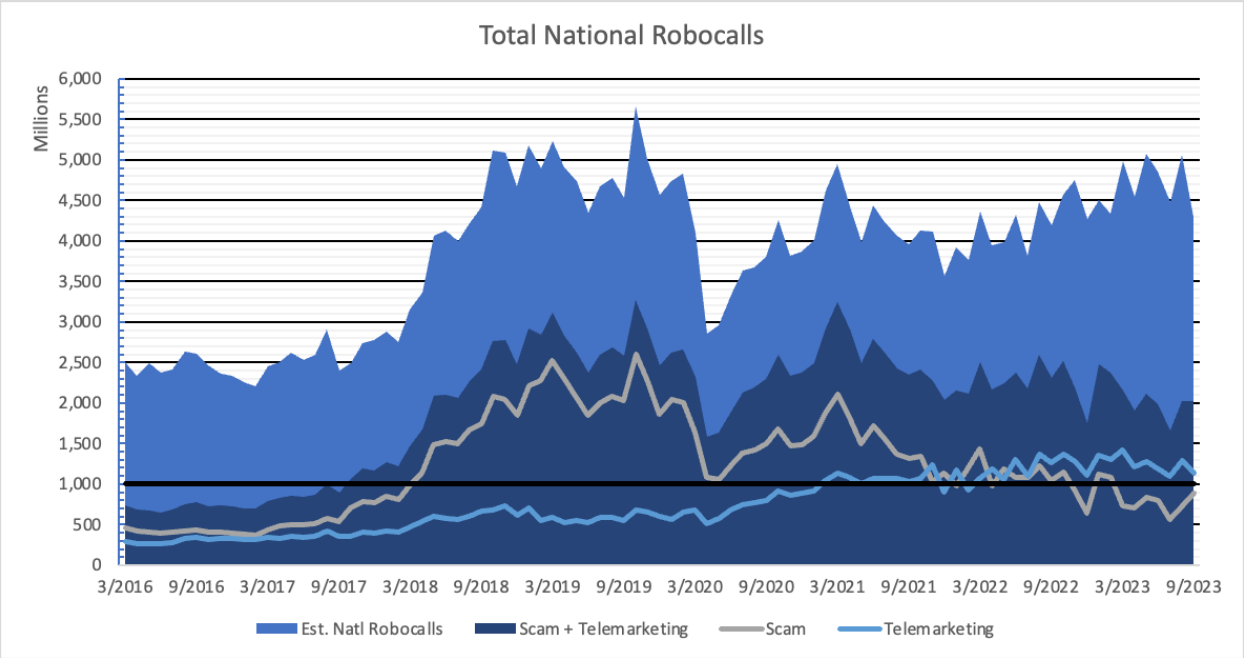
[6] Scam Robocalls report, *supra* note 2, at 6 (noting annual scam robocall volumes between 20 billion and 25 billion from 2019-2021). *See* Total National Robocalls chart, *infra*.

[7] The ITG, run by USTelcom/The Broadband Association, is designated by the FCC to determine the source of illegal calls. "The origination, delivery, and termination of robocalls involves numerous voice service providers in a complex ecosystem. Using a secure traceback portal developed by the ITG, suspected illegal robocalls are traced systematically back through various networks until the ITG identifies the originator of the suspicious calls, where the calls entered the United States if internationally originated, and often the identity of the calling party. The ITG traces the call back from the recipient to the caller – usually routing through four or more, or sometimes as many as nine or ten service providers (or "hops") across the globe." Industry Traceback Group, How a Traceback Works, *available at* https://tracebacks.org/for-government/.

[8] *See* Press Release, Federal Commc'ns Comm'n, FCC & State Attorneys General Warn Consumers of Increased Risk of Student Loan Debt Scam Robocalls and Robotexts (June 30, 2023, *available at* https://www.fcc.gov/document/fcc-state-ags-warn-student-loan-debt-scam-robocalls-robotexts; Industry

illustrates that, even as one scam or telemarketing caller or complicit provider is removed from the network, another quickly steps into its place.

Moreover, because of the complete lack of meaningful caller ID used by these callers, it remains effectively impossible for consumers to determine the difference between scam calls and unwanted spam telemarketing calls on the one hand, and legitimate calls on the other hand. Both types of unwanted calls continue to flood the system, and they all purport to be local. As it is highly doubtful that consumers have consented to receive over a billion telemarketing calls every month, most are likely illegal. The dark blue area on the chart below shows the combined volume of both scam and telemarketing calls.[9]



Traceback Group, ITG 2022 Year-In-Review: State of Industry Traceback, *available at* https://tracebacks.org/wp-content/uploads/2023/03/ITG-2022-Year-in-Review-State-of-Industry-Traceback.pdf ("Over 500 offending callers kicked off the network. Terminated callers responsible for approximately 32 million daily illegal robocalls.").

[9]All data comes from YouMail. The most recent data, which was supplied to us on October 17, 2023, was combined with publicly available data for previous time periods. Scam and telemarketing stats are likely conservative estimates based on known percentages rather than direct reporting, which would result in underreported volume on these categorizations. In the past, YouMail has cautioned that "[s]ome 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), *available at* https://www.prnewswire.com/news-releases/robocalls-top-50-3-billion-in-2022--matching-2021-call-volumes-despite-enforcement-efforts-301714297.html (quoting YouMail press release).

Americans continue to lose vast sums to scam calls and texts. The Harris Poll/TrueCaller survey found that the number of Americans who lost money through telephone scams continued to escalate in 2022, increasing from 59 million people suffering these losses in 2021 to over 68 million in 2022. As more people were scammed, the total consumer losses also increased to over $39 billion last year.[10] The FTC also reported a significant increase in individual reported losses between 2021 and 2022.[11] A March 2023 report issued by Juniper Research predicts that fraudulent robocalls will cost mobile subscribers $58 billion this year.[12]

Incessant unwanted calls and texts are degrading the value of the U.S. telephone system. The continued onslaught of unwanted calls from unknown numbers undermines the value of the entire telephone system, and makes it more difficult to reach people in emergencies because they do not answer calls.[13] As the Commission recently noted:

> . . . [T]he evidence reveals that the escalating problem of robocalls has undermined consumers' trust and willingness to rely on their landline telephone, leading consumers in many cases to simply not answer the phone. That communication breakdown can have significant health and safety of life implications for the many consumers who rely on residential landline service.[14]

---

[10] Truecaller, Truecaller Insights 2022 U.S. Spam & Scam Report (May 24, 2022), *available at* https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report.

[11] Losses from phone scams reported to the FTC by consumers increased from $700M to $798M from 2021-22, and losses from text scams more than doubled from $131M to $326M. FTC Consumer Sentinel Network, Fraud Reports by Contact Method, Reports & Amount Lost by Contact Method (Losses & Contact Method tab, with quarters 1 through 4 checked for 2021, 2022) (last visited Mar. 10, 2023), *available at* https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts. These numbers represent live scams as well as robocalls. As the number of complaints received has decreased, this means the average reported losses are getting larger.

[12] Press Release, Juniper Research, Fraudulent Robocalls to Cost Mobile Subscribers a Record $58 Billion Globally This Year, Finds Juniper Research Study (Mar. 20, 2023), *available at* https://www.juniperresearch.com/pressreleases/fraudulent-robocalls-to-cost-mobile-subscribers?utm_source=juniper_pr&utm_campaign=pr1_robocallmitigation_providers_operators_mar23&utm_medium=e ("Despite the ongoing development of robocalling mitigation frameworks, such as STIR/SHAKEN in North America, the report predicts that fraudsters' ability to innovate fraud methods will drive these losses to reach $70 billion globally by 2027. STIR/SHAKEN includes standards to mitigate fraudulent methods popular in North America, such as caller ID spoofing, which imitates a legitimate enterprise through the use of temporary business numbers.").

[13] *See* Benjamin Siegel, Dr. Mark Adbelmalek, & Dr. Jay Bhatt, ABC News, *Coronavirus Contact Tracers' Nemeses: People Who Don't Answer Their Phones* (May 15, 2020), *available at* https://abcnews.go.com/Health/coronavirus-contact-tracers-nemeses-people-answer-phones/story?id=70693586. *See also* Stephen Simpson, *Few Picking Up Phone When Virus Tracers Call*, Arkansas Democrat Gazelle, July 10, 2020, *available at* https://www.arkansasonline.com/news/2020/jul/10/few-picking-up-phone-when-virus-tracers-call/.

[14] Federal Commc'ns Comm'n, Final Rule, Limits on Exempted Calls Under the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, 88 Fed. Reg. 3668, at ¶ 21 (Jan. 20, 2023), *available at* https://www.govinfo.gov/content/pkg/FR-2023-01-20/pdf/2023-00635.pdf.

Government agencies and their contractors (such as ITG and YouMail) typically focus on scam calls, as they are the most damaging to both the recipients and the network. We understand that originating providers have increasingly resisted traceback requests from the ITG regarding telemarketing calls, claiming that these calls are legal because the recipients have provided TCPA-compliant consent for these calls. Yet it is impossible to believe that legitimate consent has been provided by subscribers for over a billion telemarketing calls each month. To address this confusion, in this past year we have been advocating that the FCC provide guidance concerning its regulations in a way that should radically reduce the number of telemarketing calls for which consent can be claimed to have been provided. Section III explains this advocacy.

FCC enforcement actions are not sufficient to make a meaningful difference in these illegal calls. U.S.-based providers continue to spurn the Commission's requirements to respond to traceback requests, as the FCC reports each year,[15] and as recently as Q2 2023.[16] Its "first-ever" robo-blocking order (issued more than three years after the passage of the TRACED Act)[17] has already been breached.[18] Traceback requests unearth gateway providers and point of entry providers (the providers who bring the calls into the US phone network) that months earlier were subject to FCC cease and desist orders for transmitting illegal robocalls.[19] Of the more than 7,000 voice service

---

[15] *Compare* Federal Commc'ns Comm'n, Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, Attachment A, "Non-Responsive 2022" tab (Dec. 23, 2022), *available at* https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2022-congress [hereinafter FCC 2022 Report to Congress] *with* Federal Commc'ns Comm'n, Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, Attachment A, "2021 NR Providers" tab (Dec. 22, 2021), *available at* https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2021-congress [hereinafter FCC 2021 Report to Congress] *with* Federal Commc'ns Comm'n, Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, Attachment D, "2020 NR Providers" tab (Dec. 23, 2020), *available at* https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2020-congress [hereinafter FCC 2020 Report to Congress].

[16] Federal Commc'ns Comm'n, Report on Traceback Data for the Period of April 2023 Through June 30, 2023) (Sept. 29, 2023), *available at* https://www.fcc.gov/document/fcc-releases-traceback-transparency-report [hereinafter Traceback Transparency report].

[17] Press Release, Federal Commc'ns Comm'n, FCC Orders Blocking of Calls from Gateway Facilitator of Illegal Robocalls from Overseas (May 11, 2023), *available at* https://www.fcc.gov/document/fcc-issues-first-ever-roboblocking-order-against-one-eye [hereinafter Blocking of Calls order].

[18] Traceback Transparency report, *supra* note 16, at 10, Traceback ID 13726; this call was in violation of the Commission's May 11 Blocking of Calls order, *supra* note 17.

[19] *See* Letter from FCC Enforcement Bureau to Jeff Lawson, CEO of Twilio Inc. and Mellissa Blassingame, Senior Director of Twilio (Jan. 24, 2023), *available at* https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-twilio; Letter from FCC Enforcement Bureau to Brittany Reed, President of SIPphony L.L.C. (Jan. 11, 2023), *available at* https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-sipphony; Letter

providers with certifications in the Robocall Mitigation Database (RMD),[20] the FCC has brought a total of 27 enforcement actions for deficient certifications; many of these actions addressed providers' failure to upload relevant documents rather than actual sub-standard practices.[21] The fines issued against some of the most egregious fraudsters[22] have not been recovered, which undermines the intended deterrent effect of imposing these fines. Yet the Commission has referred only three forfeiture orders to the Department of Justice related to unwanted calls since the FCC began TRACED Act reporting in 2020.[23]

As is described in this testimony, we believe that additional measures are necessary to protect Americans from the illegal calls.

---

from FCC Enforcement Bureau to Corey Seaman, CEO of Vultik Inc. (Jan. 11, 2023), *available at* https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-vultik-inc; Letter from FCC Enforcement Bureau to Aaron Leon, Co-Founder & CEO of thinQ Technologies, Inc. (Mar. 22, 2022), *available at* https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-thinq.

[20] Federal Commc'ns Comm'n, Robocall Mitigation Database, *available at* https://fccprod.servicenowservices.com/rmd?id=rmd_listings.

[21] *See* Press Release, Federal Commc'ns Comm'n, FCC Seeks to Remove Companies from Key Database for Non-Compliance with Anti-Robocall Rules (Oct. 16, 2022), *available at* https://www.fcc.gov/document/fcc-seeks-remove-companies-robocall-mitigation-database; Press Release, Federal Commc'ns Comm'n, FCC Plans to Remove Companies from Key Database for Non-Compliance with Anti-Robocall Rules (Oct. 3, 2022), *available at* https://www.fcc.gov/document/fcc-remove-companies-robocall-database-non-compliance.

[22] *See* Press Release, Federal Commc'ns Comm'n, FCC Proposes Record $225 Million Fine for Massive Spoofed Robocall Campaign Selling Health Insurance (June 9, 2020), *available at* https://www.fcc.gov/document/fcc-proposes-record-225-million-fine-1-billion-spoofed-robocalls-0 (proposed in June 2020), Press Release, Federal Commc'ns Comm'n, Health Insurance Telemarketer Faces Record FCC Fine of $225 Million for Spoofed Robocalls (Mar, 17, 2021), *available at* https://www.fcc.gov/document/fcc-fines-telemarketer-225-million-spoofed-robocalls (adopted in March 2021), Press Release, Federal Commc'ns Comm'n, FCC Reaffirms $225 Million Spoofed Robocall Fine (June 7, 2023), *available at* https://www.fcc.gov/document/fcc-reaffirms-225-million-spoofed-robocall-fine-against-rising-eagle (reaffirmed in June 2023). *See also* Press Release, Federal Commc'ns Comm'n, FCC Imposes Record Penalty Against Transnational Illegal Robocalling Operation (Aug. 3, 2023), *available at* https://www.fcc.gov/document/fcc-imposes-record-fine-transnational-illegal-robocalling-operation (issued after the Ohio Attorney General brought the following case in July 2022: Complaint for Permanent Injunction, Damages, and Other Equitable Relief, State of Ohio *ex rel.* Attorney General Dave Yost v. Jones, No. 2:22-cv-2700 (S.D. Ohio July 7, 2022), *available at* https://www.ohioattorneygeneral.gov/Files/Briefing-Room/News-Releases/Time-Stamped-Complaint-22-CV-2700-State-of-Ohio-v.aspx).

[23] *See* FCC 2022 Report to Congress, *supra* note 15, at 7 (continuing the trend from 2021); FCC 2021 Report to Congress, *supra* note 15, at 8, and FCC 2020 Report to Congress, *supra* note 15, at 7.

II. The FCC should establish a system to suspend complicit voice service providers after one notice, preventing them from transmitting illegal calls.

There are currently insufficient deterrents to counter the $1 million in monthly revenue[24] earned by complicit providers that transmit the one billion or more illegal calls made monthly.[25] Under the current rules, the profit from these calls clearly makes it worthwhile for providers to run the risk of transmitting the calls. Yet the income to providers pales when compared to the approximately $3 billion stolen every month from consumers through these fraudulent robocalls.[26]

Scam robocalls are transmitted as the result of the choices made by telecommunication service providers regarding what calls they will accept and transmit. Providers receive a payment for each call they transmit.

Robocalls typically follow a multi-step path from a caller to the called party, passed along from one provider to another multiple times. Calls go first to an originating provider (or a "gateway provider" in the case of a call from another country). That provider makes a choice whether to accept the calls from that caller. If it accepts the calls, it will send them to an intermediate provider that chooses to accept and transmit those calls down the call path. If that first intermediate provider decides not to accept the calls from the originating provider, the scam calls are stopped at that point and do not reach the called party unless the originating provider finds another intermediate provider willing to take them. Similarly, each hop in the chain to a subsequent intermediate provider or the terminating provider represents a separate decision by the downstream provider to accept and

---

[24] By some estimates, robocallers can send one million calls for as cheaply as $1,000 in call transmission costs; at a cost of $0.001 per call, more than one billion scam robocalls every month means that providers earn more than $1 million in revenue every month. *See, e.g., In re* Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Comments of ZipDX LLC, 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 2 (filed Aug. 17, 2022), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/108182676204994.

[25] Every month there are an average of one billion scam robocalls made to U.S. telephones, and a comparable number of illegal telemarketing calls. PR Newswire, Robocalls Top 50.3 Billion in 2022, Matching 2021 Call Volumes Despite Enforcement Efforts (Jan. 5, 2023), *available at* https://www.prnewswire.com/news-releases/robocalls-top-50-3-billion-in-2022--matching-2021-call-volumes-despite-enforcement-efforts-301714297.html (quoting YouMail press release) (scam calls made up roughly 41% of all robocall volume in 2022). The distinction between the two appears to be somewhat fluid, as they depend on how the calls are classified. The universally-reviled calls selling auto warranties—recently targeted by the Ohio Attorney General and the Commission, *see* Press Release, Office of the Ohio Attorney General, Yost Files Suit Alleging Massive Robocall Scheme (June 7, 2022)—are considered telemarketing calls, not outright scam calls. Conversation with Mike Rudolph, CTO, YouMail (Aug. 29, 2022).

[26] In May 2022, HarrisPoll, in a survey commissioned by Truecaller, estimated $39.5 billion in consumer losses over the past twelve months. *See* Truecaller, Truecaller Insights 2022 U.S. Spam & Scam Report (May 24, 2022), *available at* https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report (last visited Sept. 16, 2022). This is an average of more than $3.29 billion in consumer losses per month.

transmit those calls or to block them. Currently, the primary determinant for many of these instantaneous decisions made by the providers in the call path is profit. That must change.

As we describe in Section IV, there are tools currently available that allow providers to identify and then block scam robocalls. But providers need to be incentivized to use these tools and to block the calls found to be illegal.

The choices that providers in the call path make about whether to accept calls from upstream providers should be guided not only by the price paid for those calls, but also by the risk involved in accepting calls from those upstream providers. The consequences of the wrong choice should be steep. Providers who might otherwise be tempted to be complicit in transmitting scam calls will be financially motivated to comply with the law if punishments are swift, certain, and sufficiently severe. Given the proper incentives, the communications industry in the United States will develop and implement additional successful mechanisms as they become necessary.

Telephone providers should be incentivized to develop and use procedures to guard against transmitting fraud robocalls. For originating, gateway, and first intermediate providers specifically, there is little excuse for continuing to transmit scam robocall traffic after any notice that the traffic is illegal based on previous tracebacks, FCC or FTC notices or cease and desist letters, similar notices from state attorneys general, or notices from service providers such as YouMail.

The FCC established the Robocall Mitigation Database (RMD) as a way to keep track of voice service providers and apply requirements to them.[27] The RMD provides a powerful and effective tool to the FCC to control non-compliant providers, as providers are prohibited from accepting traffic from voice service providers that have not submitted proper certification to the RMD.[28]

We believe that the FCC should be empowered to use immediate—but temporary—suspension[29] from its Robocall Mitigation Database as a mechanism to protect telephone subscribers

---

[27] *See* Federal Commc'ns Comm'n, Robocall Mitigation Database, *available at* https://www.fcc.gov/robocall-mitigation-database.

[28] *See* 47 C.F.R. § 64.6305(e)(1). *See also In re* Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97, at ¶ 8 (Rel. Mar. 17 2023), *available at* https://docs.fcc.gov/public/attachments/FCC-23-18A1.pdf.

[29] Suspension should result in legally effective removal from the RMD. This can be accomplished via 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., Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, at ¶ 64 (filed Dec. 7, 2021), *available at* https://www.fcc.gov/ecfs/document/12080110629539/1 ("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

from receiving illegal calls, pending investigations and due process determinations. This would prioritize protecting U.S. telephone subscribers from criminal scam calls over providing originating and gateway providers access to the U.S. telephone network.[30] Once a provider has been notified by any of the government enforcement agencies, or their service providers, that it has been found to be transmitting illegal calls, such notification should serve as legal notice that the next time it is determined to be transmitting illegal calls, it will be suspended from the RMD. These suspensions should be temporary and short-lived, but immediate, pending a due process review. The due process review would determine whether this latest finding that the provider was transmitting illegal calls was a mistake that will not be repeated, or whether it justifies permanent removal from the RMD.

We have recommended this type of immediate suspension to the Commission as a way of swiftly preventing complicit voice service providers from continuing to transmit tens of thousands of illegal calls.[31] The interests of American subscribers to be protected from dangerous, fraudulent, and invasive calls would be prioritized.

We understand that this type of immediate suspension raises due process concerns for the affected providers. However, as we explain, those due process issues can be addressed.

---

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.").

[30] Most, if not all, of the offending voice service providers are VoIP (Voice over Internet Protocol) services. VoIP is a technology that accesses the telephone network through the internet, and is commonly used by many large telecommunications providers in place of traditional landlines to provide service to residential and business customers. Often, the telephone service is paired with internet access and cable television service. The VoIP providers that process the illegal robocalls are generally small, often simply 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. *See* FCC 2021 Report to Congress, *supra* note 15, at 12 ("The Commission's experience tracing back the origins of unlawful call traffic indicates that a disproportionately large number of calls originate from Voice over Internet Protocol (VoIP) providers, particularly non-interconnected VoIP providers. Moreover, the Industry Traceback Group has found that high-volume, rapid-fire calling is a cost-effective way to find susceptible targets, although it does not collect data about which robocall originators are VoIP providers.").

[31] *In re* Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Comments of Electronic Privacy Information Center and National Consumer Law Center on Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97 (filed Aug. 17, 2022), *available at* https://www.fcc.gov/ecfs/document/10817350228611/1. Our proposal for the immediate suspension of complicit providers contrasts with the Commission's procedure of issuing a Notification of Suspected Illegal Traffic, followed by an Initial Determination Order, then followed by a Final Determination Order, see FNPRM at ¶ 30. All three of those steps are required by the FCC before the provider is stopped from continuing to transmit illegal calls. In the time between the first and third steps, tens of thousands of illegal calls will reach subscribers.

Due process principles raise two concerns: 1) the timing and the content of notice given to the provider before the suspension from the RMD occurs; and 2) the opportunity for the provider to be heard and contest the factual basis for the suspension.[32]

The Commission can establish an expedited process of suspending providers from the RMD akin to the procedures established by Rule 65 of the Federal Rules of Civil Procedure for a court to provide a Temporary Restraining Order (TRO). TROs recognize the need to move quickly and without prior notice to the respondent to protect the moving party from immediate, irreparable harm.[33]

The Supreme Court has noted that "due process is flexible and calls for such procedural protections as the particular situation demands."[34] 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 known criminals who seek to defraud them prevents irreparable harm and justifies a truncated procedure that provides notice to the provider of the suspension simultaneously with initiating an immediate suspension from the RMD. The U.S. government has an interest in protecting its residents from scam calls. The Supreme Court has recognized that the government's interests are to be balanced against the private interest affected by the action—in this case, the provider's removal from the RMD and subsequent inability to transmit calls into the network.[35]

---

[32] *See, e.g.,* Mathews v. Eldridge, 424 U.S. 319, 332, 96 S. Ct. 893, 47 L. Ed. 2d 18 (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.").

[33] *See* "Legal Information Institute, Temporary Restraining Order, *available at* https://www.law.cornell.edu/wex/temporary_restraining_order (last accessed Oct. 19, 2023).

[34] Morrissey v. Brewer, 408 U.S. 471, 481, 92 S. Ct. 2593, 33 L. Ed. 2d 484 (1972). *See also* Mathews v. Eldridge, 424 U.S. 319, 349, 96 S. Ct. 893, 47 L. Ed. 2d 18 (1976) ("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.").

[35] *See* Mathews, 424 U.S. at 334-35 ("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)).

Formal Notice. Just as when a TRO is issued by a court, the system we propose would require the Commission to 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 would 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.[36] The traceback request is sent up through the call-path from the terminating provider, through the multiple intermediate providers, up to the originating or gateway providers. Not all these providers in the call path are complicit, as the illegal calls become mixed with legal calls as they travel—making it difficult for downstream providers to root out the illegal calls.

In the future, all traceback requests could include a warning that the failure to cease making illegal calls after notice, could trigger suspension from the RMD. The pre-suspension notice could also be included in notices from state attorneys general and the Federal Trade Commission. Providing notice of the *possibility* of suspension to all providers who are found to have transmitted illegal calls serves to remind every one of the potential ramifications of continuing the illegal activity.

Triggering Activity. Providers are complicit in transmitting illegal calls when they have received notice that their calls are illegal from any one of a number of enforcement agencies or their partners in this system and yet continue to pass along this traffic. Other federal agencies are engaged in battling the scam calls, including the FTC and the Social Security Administration, as are the attorneys general in most states. Additionally, responsible intermediate providers currently alert upstream providers that they are transmitting illegal calls, as do some private service providers (such as YouMail and ZipDX) that are engaged in network monitoring. In the future, the Commission

[36] Each traceback notice sent to every provider in the call path contains a text description of the call, typically explaining what makes it illegal. *See* 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 ¶¶ 93-94 and 34 ¶¶ 98-99 (M.D.N.C. Jan. 25, 2022), *available at* https://ncdoj.gov/wp-content/uploads/2022/01/FILED-Complaint_NC-v-Articul8_22-cv-00058-MDNC-2022.pdf [hereinafter North Carolina v. Articul8 Complaint].

could establish a system under which any one of these entities—state attorneys general, the FTC and other federal agencies involved in this work, intermediate providers, and private service providers—could alert the Commission when originating or gateway providers continue to transmit illegal calls even after repeated notice from any one or more of these entities. Alerts from any one of these trusted sources to the FCC could serve as the basis for the FCC to initiate immediately the suspension process. Once a trusted source provides information to the FCC regarding ongoing transmission of illegal calls by a provider, along with proof (information about the number and type of the calls, and the nature of the previous notice provided by the trusted source), that would trigger the immediate suspension notice from the FCC. At that point, the FCC would initiate the suspension of the targeted provider for a period of 10 days, by the end of which there would be a hearing to determine whether the provider would remain suspended from the RMD.

Opportunity to be Heard. Once a provider is given the formal notice 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.

We have advocated that the Commission should establish a mechanism to allow this type of fact-finding proceeding, possibly before a Commission Administrative Law Judge,[37] 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.[38] 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 . . . .[39]

---

[37] Fed. Commc'ns Comm'n, Administrative Law Judges, *available at* https://www.fcc.gov/administrative-law-judges (last accessed Oct. 19, 2023)

[38] *See* Mathews v. Eldridge, 424 U.S. 319, 334, 343-44, 96 S. Ct. 893, 47 L. Ed. 2d 18 (1976).

[39] *Id.* at 347.

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."[40] 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."[41] 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, and the billions stolen from American subscribers through these calls.

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 provide 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."[42] The Commission has already made clear in numerous instances that providers must comply with its rules, and it has listed potential consequences for failing to do so, explicitly including suspension from the RMD.[43]

---

[40] *Id.* at 349.

[41] *Id.*

[42] *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 (May 19, 2022).

[43] 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), *available at* https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf. Also, the Commission has required that providers 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, Federal Commc'ns Comm'n, FCC to Robocallers: There Will Be No More Warnings (May 1, 2020), *available at* https://docs.fcc.gov/public/attachments/DOC-364109A1.pdf.

If the Commission believes that it does not have the authority to exercise these immediate but temporary suspensions to protect American telephone subscribers from these illegal calls, we urge Congress to provide such authority.

III. The Commission should issue guidance confirming that its current regulations limit agreements for prior express consent and prior express invitation to calls from one seller, and that the E-Sign Act applies to agreements entered online.

The misuse of consumers' "consents" by lead generators and others is a major factor contributing to the increasing number of illegal telemarketing calls and texts. The number of telemarketing calls has been steadily rising in recent years, peaking at over 1.4 billion a month in March 2023.[44]

Lead generators, a common feature on the internet, refer potential customers to vendors.[45] The "leads"—the telephone numbers and other data regarding potential customers—are sold directly to sellers of products or services (such as lenders or insurance companies) or to lead aggregators that then sell the leads to sellers.[46] As courts and the FTC have noted, it is not always apparent from a particular website that it is operated by a lead generator rather than an actual lender or seller of other products or services,[47] and misrepresentations and outright consent fraud on lead generators' sites are common.[48]

---

[44] PR Newswire, U.S. Consumers Received Roughly 5 Billion Robocalls in March, According to YouMail Robocall Index: National Monthly Robocall Volume Reached Highest Peak Since November 2019 (Apr. 7, 2023), *available at* https://www.prnewswire.com/news-releases/us-consumers-received-roughly-5-billion-robocalls-in-march-according-to-youmail-robocall-index-301792292.html.

[45] *See* Federal Trade Comm'n, "Follow the Lead" Workshop, Staff Perspective (Sept. 2016), *available at* www.ftc.gov (overview of lead generation industry).

[46] *Id.* at 2 ("A lead is someone who has indicated—directly or indirectly—interest in buying a product.").

[47] *See, e.g.,* CFPB v. D & D Mktg., 2016 WL 8849698, at *1 (C.D. Cal. Nov. 17, 2016).

[48] *See* Federal Trade Comm'n, Follow the Lead Workshop—Staff Perspective 5 (Sept. 2016), *available at* www.ftc.gov. *See also* Consumer Fin. Prot. Bureau v. RD Legal Funding, L.L.C., 332 F. Supp. 3d 729, 782–783 (S.D.N.Y. 2018); MacDonald v. CashCall, Inc., 2017 WL 1536427, at *12 (D.N.J. Apr. 28, 2017), *aff'd on other grounds*, 883 F.3d 220 (3d Cir. 2018) (affirming denial of arbitration motion); CFPB v. D & D Mktg., 2016 WL 8849698, at *1 (C.D. Cal. Nov. 17, 2016); Consumer Fin. Prot. Bureau v. CashCall, Inc., 2016 WL 4820635, at *10 (C.D. Cal. Aug. 31, 2016). *See also* McCurley v. Royal Seas Cruises, Inc., 21-55099, 2022 WL 1012471 at *3 (9th Cir. Apr. 5, 2022) ("The amount of mismatched data in the record cannot all be explained by data-entry errors or family members with different last names….These facts, in combination with the evidence of widespread TCPA violations in the cruise industry, would support a finding that Royal Seas knew facts that should have led it to investigate Prospects's work for TCPA violations.").

Consumers who visit a lead generator's site are typically invited to enter their contact information into a form or application on the site. Typically, the consumer is asked to click on a link that includes language in tiny font[49] that does not anywhere indicate that the lead generator is planning to use that click to justify telemarketing calls from hundreds—or even—thousands—of telemarketers.[50]

The site operator then sells the consumer's information to interested lenders or sellers, sometimes with some level of data analysis, and often through an automated auction. A 2011 survey found that leads are sometimes sold for over $100[51]; more recent online data indicates that leads can be sold for as much as $600 each.[52]

One organization of lead generators admitted in its comments to the Commission in a March 2023 Notice of Proposed Rulemaking that lead generators are responsible for a "meaningful percentage" of entirely fabricated consent agreements.[53] These comments provide particularly helpful information about how the lead generator industry works to facilitate telemarketing robocalls: "once the consumer has submitted the consent form the company seeks to profit by reselling the 'lead' multiple—perhaps hundreds—of times over a limitless period of time. Since express written consent does not expire, the website is free to sell the consent forever."[54]

Each party that owns the consent, including the original lead generator and every subsequent purchaser of the consent, "is free to sell it again."[55] As the lead generators explain: the result of all

---

[49] For example: By clicking "Get My Auto Quotes" the consumer is supposedly agreeing that the lead generator can "share my information to the providers in our network for the purpose of providing me with information about their financial services and products." But to see the full list of callers and other lead generators that this website could sell the consumer's lead to, one must place their mouse and hover over a link embedded in the long paragraph under the place to be clicked, described *infra* at 50.

To access this form, a person must go to QuoteWizard's website at https://www.quotewizard.com/ and provide information about the insurance product they seek, as well as their name, address, and telephone number, birth date, and other personal information.

[50] *See, e.g.,* the list of thousands of insurance carrier partners of QuoteWizard, *available at* https://quotewizard.usnews.com/form/static/corp/providers.html?bn=U.S.%20News&bf=usnews.

[51] Consumer Federation of America, CFA Survey of Online Payday Loan Websites 7 (Aug. 2011), *available at* https://consumerfed.org/pdfs/CFAsurveyInternetPaydayLoanWebsites.pdf.

[52] *See* Leads Hook, Blog post, *How to Make Money Selling Leads in 2023 (& How Much to Charge)* (July 12, 2023), *available at* https://www.leadshook.com/blog/how-to-sell-leads/.

[53] Comment of Responsible Enterprises Against Consumer Harassment, CG Dockets Nos. 21-402, 02-278, at 1 (filed May 9, 2023), *available at* https://www.fcc.gov/ecfs/document/10509951114134/1.

[54] *Id.* at 3 (emphasis added).

[55] *Id.* at 6 (emphasis added).

these sales is that "[e]ach time the website operator—or an intermediary "aggregator" . . . sells the consumer's data a new set of phone calls will be made to the consumer."[56]

Additional comments in the FCC's proceeding support the point that the practice of lead generators sharing consents is a major contributing factor in the proliferation of unwanted telemarketing calls:

- The known fact that one click can sign up a consumer to thousands of businesses, related or not, is a dreadful problem. Aged leads are also problematic because, currently, consent never expires.[57]

- Until lead buyers stop purchasing non-compliant leads there will be incentives that lead to bad practices.[58]

On the other hand, comments from the telemarketing industry and lead generators defend the sharing of consumer consents with hundreds, and even thousands, of callers. For example, a trade association for telemarketers argues against the Commission's proposal in the NPRM: "It is easy to say that 1,000 companies are too many but there are many markets, such as insurance, where hundreds of relevant companies provide differentiated products."[59] The level of objections to the FCC's concerns by the lead generator industry underscores the extent to which that industry is responsible for so many of the billion monthly telemarketing calls made to American telephones.

FCC regulations already require consumers' written consents to apply to just one seller and to be non-transferable. The Telephone Consumer Protection Act[60] requires the FCC to establish regulations governing telemarketing calls. For the past several decades, the FCC's regulations have outlined explicit requirements for callers before they can make prerecorded telemarketing calls to cell phones and residential lines,[61] or any calls to lines registered on the nation's Do Not Call (DNC) Registry.[62] Both regulations require that, before those calls can be

---

[56] *Id.* at 3 (emphasis added).

[57] Comment of Drips, CG Dockets Nos. 21-402, 02-278 (filed May 8, 2023), *available at* https://www.fcc.gov/ecfs/document/10509043191182/1.

[58] Comment of National Association of Mutual Insurance, CG Dockets Nos. 21-402, 02-278 (filed May 8, 2023), *available at* https://www.fcc.gov/ecfs/document/10508029328611/1.

[59] Comment of Professional Associations for Customer Engagement, CG Dockets Nos. 21-402, 02-278, at 9 (filed May 8, 2023), *available at* https://www.fcc.gov/ecfs/document/1050879833281/1.

[60] 47 U.S.C. §§ 227 *et seq.*

[61] 47 C.F.R. § 64.1200(f)(9).

[62] 47 C.F.R. § 64.1200(c)(2)(ii).

made, the recipient must have signed an express written agreement consenting to telemarketing calls by or on behalf of a single seller.[63]

The requirements for consent or invitation to receive telemarketing calls in the current FCC regulations are quite specific, and they have been the law for a long time.[64] The current regulations prohibit telemarketing calls to a line registered on the DNC Registry unless the telemarketer has a "personal relationship with the recipient" or the caller has the subscriber's prior express invitation or permission. The rule specifies:

> Such permission must be evidenced by a signed, written agreement between the consumer and seller which states that the consumer agrees to be contacted by this seller and includes the telephone number to which the calls may be placed; . . .[65]

The critical language in this regulation is a) the agreement must be "between the consumer and seller," and b) it must specify that the consumer agrees to be contacted by "this seller." As each agreement must be between the seller and the consumer, and each agreement must be limited to the calls from that seller, the FCC's regulation clearly prohibits any agreement from providing consent to more than one seller or consent that can be sold or transferred to another seller.

Similarly, the FCC's rules for prerecorded telemarketing calls to cell phones and residential lines requires prior express written consent,[66] which the current regulations define in 47 C.F.R. § 64.1200(f)(9) as:

> (9) The term prior express written consent means an agreement, in writing, bearing the signature of the person called that clearly authorizes the seller to deliver or cause to be delivered to the person called advertisements or telemarketing messages using an automatic telephone dialing system or an artificial or prerecorded voice, and the telephone number to which the signatory authorizes such advertisements or telemarketing messages to be delivered.

---

[63] 47 U.S.C. § 227(a)(4). The regulation makes exceptions for calls to DNC lines when the calls are on behalf of charities, and when the caller has an "established business relationship" with the recipient.

[64] The Commission's regulation governing consent for calls to DNC lines were promulgated in 2003. *See* Rules and Regulations Implementing the Telephone Consumer Protection Act (TCPA) of 1991, Final Rule, CG Docket No. 02-278, 68 Fed. Reg. 44,144, 44,148 ¶ 22 (F.C.C. July 25, 2003) ("Consistent with the FTC's determination, we conclude that for purposes of the national do-not-call list such express permission must be evidenced only by a signed, written agreement between the consumer and the seller which states that the consumer agrees to be contacted by this seller, including the telephone number to which the calls may be placed." (emphasis added)). The regulations requiring prior express written consent for prerecorded telemarketing calls to residential lines and cell phones were promulgated in 2012. *See In re* Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991, Report and Order, Docket No. 02-278, 27 F.C.C. Rcd. 1830, 1873 ¶ 28 (F.C.C. Feb. 15, 2012).

[65] 47 C.F.R. § 64.1200(c)(2)(ii) (emphasis added).

[66] 47 C.F.R. § 64.1200(a)(3).

> (i) The written agreement shall include a clear and conspicuous disclosure informing the person signing that:
>
> > (A) By executing the agreement, such person authorizes the seller to deliver or cause to be delivered to the signatory telemarketing calls using an automatic telephone dialing system or an artificial or prerecorded voice;[67]

Unlike the requirements for prior express invitation under 47 C.F.R. § 64.1200(c)(2)(ii) for calls to DNC lines, this regulation does not explicitly require that the agreement be "between" the person to be called and the seller. But the references to "the seller" make it clear that the agreement can permit calls from only one seller.

Thus, both of these consent provisions are explicit in allowing consent to be given to receive calls only from a single identified seller. If there were any ambiguity, the FCC's rule should be interpreted to be consistent with the parallel provisions of the Federal Trade Commission's (FTC) Telemarketing Sales Rule (TSR).[68] Congress has instructed the Commission to maximize consistency with the FTC's rules,[69] and even without a congressional directive it is obvious that inconsistent rules governing the same activity would be problematic.

The TSR's requirements that "the seller" obtain the consumer's consent, and that the consent allows delivery of prerecorded messages "by or on behalf of a specific seller," make it clear that a third party that is not the seller's agent cannot obtain the consumer's consent, and that consent cannot be sold or transferred. And the FTC has explicitly reiterated this point in its Business Guidance,[70] which explains:

> May a seller obtain a consumer's written permission to receive prerecorded messages from a third-party, such as a lead generator? No. The TSR requires the seller to

---

[67] 47 C.F.R. § 64.1200(f)(9) (emphasis added).

[68] 16 C.F.R. §§ 310.1 *et seq.* With respect to prerecorded calls, before a telemarketing call can be made, the TSR requires that the "seller [must have] obtained [consent] only after a clear and conspicuous disclosure that the purpose of the agreement is to authorize the seller to place prerecorded calls to such person; . . ." 16 C.F.R. § 310.4(b)(1)(v)(A)(i) (emphasis added).

[69] The Do-Not-Call Implementation Act, Pub. L. No. 108-10, § 3, 117 Stat. 557 (2003) ("Not later than 180 days after the date of enactment of this Act, the Federal Communications Commission shall issue a final rule pursuant to the rulemaking proceeding that it began on September 18, 2002, under the Telephone Consumer Protection Act (47 U.S.C. 227 et seq.). In issuing such rule, the Federal Communications Commission shall consult and coordinate with the Federal Trade Commission to maximize consistency with the rule promulgated by the Federal Trade Commission . . . ." (emphasis added)).

[70] Federal Trade Comm'n, Business Guidance, Complying with the Telemarketing Sales Rule, *available at* https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#prerecordedmessages.

obtain permission directly from the recipient of the call. The seller cannot rely on third-parties to obtain permission.

The FCC should simply issue guidance reiterating the clear meaning of its existing regulations. To confirm what the FCC's regulations have said for the past twenty years, and to show consistency with the FTC's rule, the FCC should similarly issue guidance that under its existing rules, consent agreements must identify a single seller and that a seller or telemarketer cannot obtain consent by purchasing it from, or obtaining a referral from, a lead generator, another seller, telemarketer, or an independent contractor.

In March 2023, the Commission proposed new regulations intended to limit the collection and selling of consent agreements among lead generators.[71] However, we—on behalf of a broad coalition of consumer and privacy groups—have strongly urged the Commission *not* to proceed with its proposed changes to its regulations, as that proposal would be a reduction in consumer protections from the current regulations, and would be inconsistent with the existing language which already addresses the problem. In extensive comments, and several meetings,[72] we have explained how the current TCPA regulations already set the necessary standards**.** Instead of issuing new regulations, we have urged the Commission to issue guidance reiterating the requirements in its current regulations, along with a reminder that the federal E-Sign law applies whenever writings or signatures are provided electronically. Our comments on these points have been reiterated by USTelecom-The Broadband Association,[73] as well as comments filed on behalf of 28 state attorneys general.[74]

---

[71] *In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Report and Order and Further Notice of Proposed Rulemaking, CG Docket Nos. 21-402, 02-278 (Rel. Mar. 17, 2023), *available at* https://www.fcc.gov/document/fcc-adopts-its-first-rules-focused-scam-texting-0. The Proposed Rule was published in the Federal Register at 88 Fed. Reg. 20,800 (Apr. 7, 2023) and is available at https://www.govinfo.gov/content/pkg/FR-2023-04-07/pdf/2023-07069.pdf.

[72] *See In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Comments of National Consumer Law Center et al., CG Docket Nos. 21-402, 02-278 (filed May 8, 2023), *available at* https://www.fcc.gov/ecfs/document/1050859496645/1 and *In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Reply Comments of National Consumer Law Center et al., CG Docket Nos. 21-402, 02-278 (filed June 6, 2023), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/10606186902940.

[73] *In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Comments of USTelecom – The Broadband Association, CG Dockets No. 21-402, 02-278 (filed May 8, 2023), *available at* https://www.fcc.gov/ecfs/document/10508915228617/1.

[74] *In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Reply Comments of 28 State Attorneys General, CG Dockets No. 21-402, 02-278 (filed June 6, 2023), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/10606091571575.

Instead of issuing new rules, the FCC should simply issue guidance to industry, reiterating that the existing rules require a consumer's consent to be limited to calls by or on behalf of a single seller, and that this consent cannot be sold or transferred. Insisting on compliance with current TCPA regulations will significantly reduce the number of unwanted telemarketing calls by limiting the sale of consent by lead generators. Most of the billion-plus monthly telemarketing calls that consumers receive today are based on consents supposedly obtained through lead generators on various websites. Yet the fact that lead generators and their telemarketing customers have been ignoring the requirements of the Commission's regulations on telemarketing calls—and getting away with it for many years—is not a reason to allow that behavior to continue. As the Commission has repeatedly recognized, it is largely because of too many robocalls that the use of the telephone has declined in recent years.[75]

Limiting the ability to use a consumer's single agreement of consent to justify multiple calls from different telemarketers will stop a large number of unwanted telemarketing calls, as only a tiny fraction of the consents previously used to justify the calls will meet the requirements. Requiring the calling and lead generation industries to comply with regulations that have been on the books for over a decade may force a change in their practices, but it will be a change that will greatly benefit consumers.

Complying with the existing rules will not prevent lead generators from putting consumers in touch with sellers they want to hear from. Nothing in the FCC's rules prevents lead generators from providing information to consumers, including direct referrals to sellers of products and services through weblinks. And nothing prohibits lead generators from providing the offered referrals through email or snail mail (addresses are often required information), or even by simply displaying the information right on the website. Many lead generators currently do not require the entry of a telephone number to refer a consumer to a seller,[76] and others ask for minimal information (like zip code) and then refer the consumer right to a seller's website.[77] All of these practices, which are far less invasive than unleashing a torrent of telemarketing calls, will be unaffected by compliance with the existing rules.

---

[75] *See* FNPRM at ¶ 1("Many of us no longer answer calls from unknown numbers and, when we do, all too often find them annoying, harassing, and possibly fraudulent. Consumers are not the only losers when this happens; legitimate callers have a hard time completing the calls consumers do want to receive.").

[76] *See, e.g.*, https://www.google.com/travel/flights.

[77] *See, e.g.,* https://best.ratepro.co/; https://www.esurance.com/; www.nerdwallet.com.

The FCC should also issue guidance reiterating that online consent agreements must comply with E-Sign. Although few parties comply, the federal E-Sign Act applies when signatures are provided electronically, and when electronic records are used to satisfy requirements for a writing. The E-Sign Act establishes the rules for satisfying a requirement for a writing or a signature with their electronic equivalents.[78]

It is only because of the E-Sign Act that an electronic action like a click on a website can carry the same legal significance as a "wet" signature.[79] As a result, an electronic click used by a telemarketer to signify a person's signature on an agreement providing express consent or invitation to receive telemarketing calls under either the TCPA regulations or the TSR will qualify as a signature that can bind the person to the agreement only if that click meets the definition of an electronic signature in the E-Sign Act at 15 U.S.C. § 7006(5). Among other things, this definition requires that the signer have the intent to sign the electronic record.[80] When the agreement is to provide consent for telemarketing calls, the place on the electronic form where the electronic action is to be applied must clearly indicate that the consumer, by taking the electronic action, is intending to sign the related electronic agreement to receive those calls. An electronic sound, symbol, or process applied on a website that is hyperlinked to a list of multiple other parties from whom the person is purportedly agreeing to receive calls should not be construed to indicate consent by the person applying the click, because the person would not have had the required intent to sign an agreement with all of the callers each and every one of the hundreds or thousands of callers included in the hyperlinked list.[81]

---

[78] 15 U.S.C. §§ 7001 *et seq.*

[79] 15 U.S.C. § 7001(a)(2).

[80] 15 U.S.C. § 7006(5) ("The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." (emphasis added)).

[81] *See, e.g.,* Federal Commc'ns Comm'n, *In re* Urth Access, Inc., Order, File No. EB-TCD-22-00034232, 2022 WL 17550566, at ¶ 16 (Rel. Dec. 8, 2022), *available at* https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls ("The websites included TCPA consent disclosures whereby the consumer agreed to receive robocalls from 'marketing partners.' These 'marketing partners' would only be visible to the consumer if the consumer clicked on a specific hyperlink to a second website that contained the names of each of 5,329 entities. We find that listing more than 5,000 'marketing partners' on a secondary website is not sufficient to demonstrate that the called parties consented to the calls from any one of these 'marketing partners.'" (footnote omitted)).

Because the telemarketing industry has routinized non-compliance with the FCC's current regulations, we have urged the FCC to issue guidance clarifying how these regulations apply to telemarketing calls.

IV. Legal callers should leverage their power in the marketplace to protect their calls from blocking and mislabeling, which will assist in the efforts to eliminate the illegal calls.

The FCC's efforts to address illegal calls include its recent proposal[82] to encourage terminating providers to block more suspicious calls, as well as continuing to label suspicious calls.[83] While supporting these proposals, we have respectfully suggested that just doing more of the same—requiring blocking of calls from FCC-identified providers, encouraging opt-out blocking and labeling, and enforcing and tweaking rules for STIR/SHAKEN authentication—seems unlikely to change the basic dynamic that drives these illegal calls: originating and gateway providers are making sufficient income from these calls to make it more profitable to keep making the calls and risking the punishment.[84] Clearly, the potential for costly consequences from conveying these illegal calls is sufficiently remote and outweighed by the income from these calls such that the current measures fail to dissuade these providers from continuing their current practices.[85]

Instead, we have urged the Commission to adopt a set of best practices for legal callers that—if widely used—will likely eliminate many of the illegal calls plaguing subscribers' telephone lines. These best practices would leverage the market power of the legal callers to change the calculus of voice service providers that are currently complicit—either knowingly or with deliberate

---

[82] FNPRM. The Proposed Rule was published in the Federal Register at 88 Fed. Reg. 43,489 (July 10, 2023) and is available at https://www.federalregister.gov/documents/2023/07/10/2023-13032/advanced-methods-to-target-and-eliminate-unlawful-robocalls.

[83] We note that call labeling should only be used in lieu of blocking when there is meaningful doubt about the legality and value of the call, such that allowing the call to go through poses less risk than blocking it. In other words, calls that appear to be likely scams should always be blocked, as the risk to consumers from those calls is significant. Blocking scam calls should be the first and primary line of defense, not labeling.

[84] *See In re* Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor, Reply Comments of National Consumer Law Center, Electronic Privacy Information Center, & Public Knowledge Relating to Seventh Report and Order and Eighth Further Notice of Proposed Rulemaking, CG Docket No. 17-59, WC Docket No. 17-97 (filed Sept. 8, 2023), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/1090831416629.

[85] 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).

blindness—about their transmission of illegal calls. If legal callers were to demand, on a uniform basis, that the voice service providers that transmit their calls must adopt the Commission's best practices and avoid transmitting illegal calls, the profit from illegal calls would plummet. Even more importantly, the illegal calls would no longer mixed with the legal calls, making it much easier for the terminating providers to identify and block these calls.

Legal callers have repeatedly complained that their legal—and often wanted—calls are erroneously blocked or labeled. As a result, subscribers are likely missing some calls that they want or need from callers,[86] and legal callers are experiencing escalating costs and frustrations with consistently and reliably completing their calls to subscribers. These problems are caused by the mislabeling and incorrect blocking of their *legal* calls.[87]

Legal callers are responsible for placing over two billion robocalls every month. While some of these calls are surely unwanted, there is no dispute that a significant percentage of these calls are desired, welcomed, or critical to their recipients (*e.g.*, school, government, security, or disaster alerts). The difficulties with reliably completing these wanted calls are apparently increasing. Legal calls are mixed with a torrent of illegal calls at shared originating and intermediating providers, causing legal calls to be tainted by illegal calls in the same call path. The result is that legal calls end up mislabeled or blocked by downstream providers seeking to protect subscribers from illegal calls.

We have proposed that the Commission facilitate leveraging the considerable marketplace power of these legal callers to assist in the efforts to eliminate dangerous and unwanted calls—scam and illegal telemarketing calls. If legal callers are armed with the information about how to avoid using the providers that are processing illegal calls, the sheer economic power of legal callers may be sufficient to force voice providers to stop transmitting illegal calls.

We have suggested that the Commission define best practices for legal callers and provide clear recommendations to enable these callers to use their power in the telephone marketplace to ensure that their calls are placed only with providers that do not originate calls or transmit from illegal callers. A market-based approach like this would a) provide strong financial incentives to originating and intermediate providers to avoid transmitting illegal calls; b) facilitate the transmission of legal calls through call paths that would eliminate the likelihood that the calls would be labeled

---

[86] *See, e.g.*, *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor, Comments of Numeracle, Inc, CG Docket No. 17-59, WC Docket No. 17-97, at 2, 19 (filed Aug. 9, 2023), *available at* https://www.fcc.gov/ecfs/document/108102252803712/1.

[87] *Id.*

improperly or blocked by downstream or terminating providers; and c) supplement the other mechanisms created by the Commission intended to address illegal calls. **The foundation of a market-based approach is providing legal callers with the information that they need to keep their calls separate from illegal calls.** As we explain below, this information is already available from private analytics-based platforms. The Commission need only lead the way.

Legal calls are mistaken for illegal calls because of the lack of transparency regarding the providers that are transmitting both types of calls. As described in Section II, *supra,* automated calls take circuitous routes from origination to the call recipient through the least-cost routing process.[88] The least-cost routing process allows downstream providers to refuse to take calls from upstream providers if they do not like the price offered for the transmittal or if they deem the calls potentially illegal—and thus too costly. The issue is how to incentivize downstream providers to refuse more of these illegal calls. The providers that are complicit in transmitting illegal calls are well aware of what they are doing. They know that the calls are illegal because they have received multiple traceback requests. With each traceback request, they are given a notice from the Industry Traceback Group (ITG) that they are transmitting suspicious calls.[89] 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.

The phone network currently allows for legal calls to be mixed with illegal calls, which frustrates attempts to identify the illegal calls accurately and label or block them. Disaggregating legitimate calls from illegal traffic is the first step to resolving both problems. To do that, legal callers need to be equipped with the means to avoid the providers transmitting high volumes of illegal traffic alongside their legal calls.

---

[88] *See* Appendix to Complaint, United States of America v. Palumbo, Case 1:20-cv-00473, Declaration of Marcy Ralston at 10-12 ¶ 22 (E.D.N.Y. Jan. 28, 2020). Marcy Ralston, a Special Agent in the Social Security Administration's Office of Inspector General, Office of Investigations, provided a sworn statement in *United States of America v. Palumbo.*

[89] Each traceback notice sent to every provider in the call path contains a text description of the call, typically explaining what makes it illegal. *See* North Carolina v. Articul8 Complaint, *supra* note 36, at 30 ¶¶ 93-94 and 34 ¶¶ 98-99. In addition, most traceback notices include a link to the recorded message that was captured. North Carolina alleged that ITG notified Articul8 of this illegal traffic 49 times for calls. *Id.* at 30 ¶ 93. In one version of the Social Security scam, "the caller says your Social Security number has been linked to a crime (often, he says it happened in Texas) involving drugs or sending money out of the country illegally." Jennifer Leach, Federal Trade Comm'n, Consumer Advice, *Fake calls about your* SSN (Dec. 12, 2018), *available at* https://consumer.ftc.gov/consumer-alerts/2018/12/fake-calls-about-your-ssn.

The results of tracebacks and government investigations into illegal providers are only reported publicly after they are completed. To protect themselves, legal callers need to know in real time which providers are responsible for illegal calls, and they need to be made aware of how to use that information to protect their calls from being mislabeled or blocked.

In their enforcement efforts, the Commission and other federal and state government agencies currently use information from non-government service providers that maintain real-time **content-based analytics** platforms. These platforms capture live evidence of illegal calls, including the content of the calls (both audio and transcribed), the telephone numbers of the callers and called parties, the date and time, the upstream voice service providers that provided STIR/SHAKEN attestation, and more. This information is aggregated to show volumes of calls, patterns in the calls, call paths, compliance with STIR/SHAKEN, and more. These content-based analytics platforms are also used by private enterprises in banking, health care, and hospitality and government agencies seeking to protect themselves from callers pretending to be these businesses to scam consumers. The platforms assist these institutions by identifying the voice service providers responsible for transmitting the imposter calls, thereby facilitating the disruption of illegal calls.[90]

There is no reason that legal callers could not use the information from these content-based analytics platforms to identify the providers responsible for transmitting illegal calls. Once aware of which providers are participating in that conduct, a legal caller could switch to another originating provider that is not associated with illegal calls. Additionally, in its contracts with the providers originating their legal calls, the legal callers could require that the provider not send this caller's traffic to immediately downstream providers that are transmitting illegal calls from upstream providers that are currently accepting bad traffic.

If sufficient numbers of legal callers employ these practices, in combination, considerable market pressure would be exerted on telecom providers to improve their mitigation efforts, as they would risk losing legal call traffic to competitors that are more effective at detecting and blocking bad traffic. Instead, at present, these originating and intermediate providers are rewarded when legal

[90] Both YouMail and ZipDX capture audio evidence and other material information on tens of thousands or millions of illegal calls daily. YouMail's solutions assist subscribers by identifying likely illegal calls, transferring those calls to voicemail, and then, with the permission of the called consumers, capturing and transcribing the content of these calls. ZipDX performs similar functions using banks of its own telephone numbers (referred to as honeypots) to receive the calls. Both platforms categorize and analyze the calls, providing extensive detail about call patterns and call paths as well as transcripts of the illegal calls. Both can also identify which telephone providers are continuing to provide STIR/SHAKEN attestations to illegal calls even after receiving notice of the bad traffic.

and illegal traffic are mixed together. That mixing masks illegal traffic, allowing the providers that are transmitting illegal traffic to continue profiting from it and further degrading the reliability of the American telephone system.

The Commission can provide information on best practices that would clarify for legal callers how to ensure that their calls are not mixed with the illegal calls. Once these best practices are adopted by legal callers, the Commission can impose additional requirements on downstream and terminating providers to step up their blocking of suspicious calls, providing further incentives to legal callers to ensure that their calls are sent on legitimate call paths. Callers will be incentivized to use this method because it will facilitate the delivery of their calls, but the Commission's expanded blocking requirements may provide an additional stimulus.

To prevent the telephone system from becoming further degraded by the prevalence of illegal, dangerous, and invasive calls, we have urged the Commission to consider recommending and facilitating these types of best practices for legal callers.

Conclusion

I very much appreciate the opportunity to provide the Committee with our ideas and proposals for how to address illegal robocalls. Please let me know if you have questions.