

JEFF JACKSON
ATTORNEY GENERAL



TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL
TNAYER@NCDOJ.GOV

April 9, 2025

Ananth Velupillai, CEO
Lingo Telecom, LLC
c/o Stephen Conley and Kevin Rupy
Wiley Rein LLP
2050 M Street NW
Washington, DC 20036

*Sent via certified mail, return receipt requested, and via email to SConley@wiley.law,
KRupy@wiley.law*

Re: SECOND AND FINAL NOTICE LETTER from the Anti-Robocall Multistate Litigation Task Force Concerning Lingo Telecom, LLC's Continued Involvement in Suspected Illegal Robocall Traffic

Dear Mr. Velupillai:

The Anti-Robocall Multistate Litigation Task Force's ("Task Force")¹ investigation of Lingo Telecom, LLC ("Lingo")² has shown that Lingo has transmitted, and continues to transmit, suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is the Task Force's second and final attempt to informally apprise you of the Task Force's concerns regarding Lingo's call traffic, and to caution Lingo that it should scrutinize the call traffic of its current customers, evaluate the efficacy of its existing robocall mitigation policies, and cease transmitting illegal traffic on behalf of its current customers.

¹ The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall ecosystem that are identified as being responsible for significant volumes of illegal and fraudulent robocall traffic routed into and across the country.

² Lingo Telecom, LLC—FCC 499 Filer ID No. 802572—"Lingo") does business under the following trade names: BullsEye; Trinsic Communications; Excel Telecommunications; Clear Choice Communications; VarTec Telecom; Impact Telecom; Startec, Americatel, and Lingo. Bullseye Telecom, Inc. is Lingo's holding company, and Lingo's parent company is Lingo Management, LLC. Lingo formerly conducted business as Matrix Telecom, LLC. Ananth Velupillai serves as Lingo's Chief Executive Officer. Vilas Uchil is Chief Operating Officer, Christopher Ramsey is Chief Revenue Officer, and Alex Valencia is Chief Compliance Officer.

The Task Force provides this Notice in order to memorialize some of its investigative findings to date.

Task Force’s Findings Regarding Lingo’s Call Traffic

As you are aware, on August 1, 2022, the Task Force issued its Civil Investigative Demand (“CID”) to Lingo to identify, investigate, and mitigate suspected illegal call traffic that is or was accepted onto, and transmitted across, Lingo’s network. On November 3, 2023, the Task Force issued a Notice to Lingo (“2023 Task Force Notice”) memorializing some of the Task Force’s findings concerning Lingo’s call traffic, informing you of the Task Force’s continuing concerns regarding its call traffic, and cautioning Lingo that it should cease transmitting any illegal traffic immediately. Based on pertinent analyses and information available to the Task Force, it appears that Lingo has continued to transmit calls associated with high-volume illegal and/or suspicious robocall campaigns.

As noted in the 2023 Task Force Notice, as part of its investigation into the transmission of illegal robocalls and the providers and entities that originate and/or route them, the Task Force regularly reviews call traffic information from several industry sources, including USTelecom’s Industry Traceback Group (“ITG”)³ and ZipDX LLC (“ZipDX”).⁴

Call traffic data from the ITG shows that it issued at least **630 traceback notices** to Lingo since January 2019 for calls it accepted and/or transmitted onto and across the U.S. telephone network. These notices from the ITG cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning SSA government imposters, financial impersonations, utility disconnects, Amazon suspicious charges, student loans, and others, with Lingo identified as serving in various roles in the call path. At least **282 traceback notices** were issued since August

³ Established in 2015, the ITG is a private collaborative industry group—composed of providers across wireline, wireless, VOIP, and cable services—that traces and identifies the sources of suspected illegal and suspicious robocalls. In December 2019, Congress enacted the Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) to combat the scourge of unlawful robocalls. *See* Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019). Following its enactment, the Federal Communications Commission designated the ITG as the official private-led traceback consortium charged with leading the voice communications industry’s efforts to trace the origin of suspected illegal robocalls through various communications networks through tracebacks. *See* 47 C.F.R. § 64.1203.

⁴ ZipDX is a provider of web- and phone-based collaboration services, which also focuses resources on developing and making technology available that is directed at mitigating illegal robocalls and other telephone-based fraud and abuse. ZipDX’s proprietary tool “RRAPTOR” is one such technology, which is an automated robocall surveillance tool that captures call recordings and information for calls largely associated with high-volume suspicious calling campaigns, and identifies the providers who have affixed their SHAKEN signatures to each of the captured calls, indicating that the provider is in the call path and whether those providers have attested to knowing the calling party who made the suspicious call and/or knowing of the calling party’s right to use that calling number to make that suspicious call. *See* ZipDX, What is RRAPTOR?, <https://legalcallsonly.org/what-is-rraptor/> (last visited Oct. 17, 2024).

2022—after the Task Force issued its CID to Lingo—and, of those, still more than **105 traceback notices** were issued since the 2023 Task Force Notice. Additionally, the traceback notices issued since August 2022 continue to show that Lingo is being identified as the point-of-entry or gateway⁵ provider for some of this traffic, as well as the immediate downstream provider to the originating provider and the originating provider itself. Because the ITG estimates that each traced call is representative of a large volume of similar illegal and/or suspicious calls,⁶ Lingo is likely continuing to cause significant volumes of illegal and/or suspicious robocalls to ultimately reach U.S. consumers, despite traceback notifications from the ITG of this identified and suspected illegal call traffic.

Information available from ZipDX indicates that Lingo also attested to calls for a number of the same high-volume robocalling campaigns for which it received and/or continues to receive traceback notices from the ITG. For instance, during the last six months, ZipDX identified **120 suspicious calls** transmitted by Lingo **from 102 unique calling numbers**,⁷ exhibiting characteristics indicative of calls that are violations of federal and state laws; 91% of these calls were also made to numbers that have been registered on the National Do Not Call Registry.⁸ Further, 100% of these calls were signed by Lingo with a C Level STIR/SHAKEN attestation, indicating that Lingo received the call without a signature. While we recognize Lingo's obligation as an intermediate provider to affix an attestation to every unsigned call that it receives, we are concerned that your upstream call source(s) are continuing to fail to affix an A- or B-attested signature of their own, and that your acceptance of these calls despite that failure is evidence of Lingo's culpability for these calls. Given the prolific nature of the calls, the Task Force is

⁵ *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, 87 FR 42916, 42917–18, para. 7 (2022) (defining a “gateway provider” as “a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider”).

⁶ USTelecom, *Industry Traceback Group Policies and Procedures*, at 4 (last revised April 2022) (*ITG Policies & Procedures*) (defining “campaign” as “[a] group of calls with identical or nearly identical messaging as determined by the content and calling patterns of the caller,” where “[a] single Campaign often represents hundreds of thousands or millions of calls”), *available at* <https://r01986.a2cdn1.secureserver.net/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf>.

⁷ The use of many unique calling numbers for this volume of called numbers indicates a suspicious pattern in your call traffic of “snowshoeing” or “snowshoe spoofing,” which is a practice often employed by illegal robocallers and telemarketers to circumvent the protections of the STIR/SHAKEN call authentication framework by using significant quantities of unique numbers for caller IDs on a short-term or rotating basis in order to evade behavioral analytics detection, or to bypass or hinder call blocking or call labeling analytics based on the origination numbers. Telephone numbers used for snowshoeing sometimes cannot themselves receive incoming calls, which has the effect of impeding an audit of the legitimacy of these calling numbers.

⁸ Most calls captured by RRAPTOR are calls made to phone numbers that have been registered on the National Do Not Call Registry.

concerned that Lingo has failed, or continues to fail, to take any proactive steps to mitigate this traffic.

On the issue of concerns regarding STIR/SHAKEN attestations, and as Lingo is well aware, on February 6, 2024, Lingo was issued a Notice of Suspected Illegal Traffic⁹ from the Federal Communications Commission (“FCC”). The FCC Notice was issued as a result of Lingo’s identified role as the originating provider for improperly attested calls that played an apparently deepfake prerecorded message from a voice that was artificially created to sound like the U.S. President advising potential Democratic voters to refrain from voting in New Hampshire’s January 2024 primary election. This matter, resolved by settlement with the FCC, resulted in a Consent Decree in which Lingo committed to implement a compliance plan and agreed to pay a \$1 million civil penalty.¹⁰

Lastly, analysis of a portion of Lingo’s likely involvement in the routing of nationwide call traffic concerning Amazon/Apple imposter robocalls was assessed. Between October 2021 and August 2024, among a nationwide sample of over 1.8 million transcribed and recorded Amazon/Apple imposter robocalls, **approximately 89,100 of these Amazon/Apple imposter robocalls are estimated to be attributable to Lingo.** Thus, of the more than 910.9 million estimated Amazon/Apple imposter robocalls reaching consumers across the country in this sample during this period, **approximately 44.5 million of these scam robocalls are estimated to be attributable to Lingo.**

A similar analysis of Lingo’s likely involvement in the routing of nationwide call traffic concerning SSA/IRS government imposter robocalls was assessed. Between January 2020 and June 2022, among a nationwide sample of over 4.68 million transcribed and recorded SSA/IRS government imposter robocalls, **more than 297,200 of these SSA/IRS government imposter robocalls are estimated to be attributable to Lingo.** Thus, of the over 2.37 billion estimated SSA/IRS government imposter robocalls reaching consumers across the country in this sample during this period, **approximately 148.6 million of these scam robocalls are estimated to be attributable to Lingo.**

After reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force has concluded that Lingo is and/or has been involved in, at a minimum, transmitting call traffic indicative of, and associated with, recurrent high-volume illegal and/or suspicious robocalling campaigns and/or practices, which conduct could subject Lingo to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and state laws.

⁹ Letter from Loyaan A. Egal, Chief, FCC Enforcement Bureau, to Alex Valencia, Chief Compliance Officer, Lingo Telecom, LLC, 2024 WL 488250 (Feb. 6, 2024), *available at* <https://www.fcc.gov/document/fcc-demands-entity-behind-nh-robocalls-stop-illegal-effort>.

¹⁰ FCC, *In re Lingo Telecom, LLC*, File No.: EB-TCD-24-00036425, Consent Decree (Aug. 21, 2024), *available at* <https://www.fcc.gov/document/fcc-settles-spoofed-ai-generated-robocalls-case>.

Overview of Select Relevant Laws

As Lingo well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,¹¹ the Telephone Consumer Protection Act,¹² and/or the Truth in Caller ID Act,¹³ as well as state consumer protection statutes.

Telemarketing Sales Rule (15 U.S.C. §§ 6101–6108; 16 C.F.R. Part 310)

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act which directed the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices.¹⁴ Pursuant to this directive, the FTC promulgated the Telemarketing Sales Rule (“TSR”). It is a violation of the TSR for voice service providers to provide substantial assistance to customers that the provider “knows or consciously avoids knowing” are engaged in practices that violate TSR provisions against deceptive and abusive telemarketing acts or practices.¹⁵ State Attorneys General have concurrent authority with the FTC to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR.¹⁶

Telephone Consumer Protection Act (47 U.S.C. § 227; 47 C.F.R. §§ 64.1200 and 64.1604)

Under the Telephone Consumer Protection Act (“TCPA”), the FCC promulgated rules restricting calls made with automated telephone dialing systems and calls delivering artificial or prerecorded voice messages.¹⁷ Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.¹⁸ State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.¹⁹ The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,²⁰ including those made with the “prior express consent” of the called party or with “prior express *written* consent” of the called party for telemarketing calls.²¹ Note, however, the FCC has found in at least one instance that single consents purportedly given

¹¹ 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4.

¹² 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

¹³ 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

¹⁴ 15 U.S.C. § 6102.

¹⁵ 16 C.F.R. § 310.3(b).

¹⁶ 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

¹⁷ 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3).

¹⁸ 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2).

¹⁹ 47 U.S.C. § 227(g)(1).

²⁰ 47 U.S.C. § 227(b)(1)(A)–(B), (b)(2)(B); 47 C.F.R. § 64.1200(a)(1)–(3), (a)(9).

²¹ 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.²²

Truth in Caller ID Act (47 U.S.C. § 227(e))

Under the federal Truth in Caller ID Act, it is generally unlawful for a person to “knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.”²³ State Attorneys General have the authority to bring enforcement actions for violations of the Truth in Caller ID Act and its prohibition against illegal caller identification spoofing.²⁴ Such violative conduct can lead to assessments of civil penalties of up to \$10,000 for each violation, or three times that amount for each day of continuing violations.²⁵ Note that any penalties for violations of the Truth in Caller ID Act are in addition to those assessed for any other penalties provided for by the TCPA.²⁶

General Note regarding State Laws

In addition to their authority to enforce the above federal statutes, State Attorneys General are empowered to enforce their respective state laws regulating various aspects of the initiation and transmission of illegal robocall and telemarketing call traffic across the U.S. telephone

²² For example, in November 2022, the FCC issued an order requiring all voice service providers to block calls from provider Urth Access, LLC. In response to allegations concerning the transmission of illegal robocalls, Urth Access claimed to have obtained express consent for each of the calls. However, that consent stemmed from websites where consumers purportedly agreed to receive robocalls from over 5,000 “marketing partners” listed on a separate site. The FCC found this type of practice insufficient to constitute express consent to the marketing partners to contact the consumers. See *FCC Orders Voice Service Providers to Block Student Loan Robocalls*, <https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls> (Order); *FCC Issues Robocall Cease-and-Desist Letter to Urth Access*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-urth-access> (Cease-and-Desist Letter). We note that this decision is consistent with the FTC’s interpretation of the express consent requirement of the TSR. See Federal Register, Vol. 73 No. 169, 2008 at 51182, <https://www.govinfo.gov/content/pkg/FR-2008-08-29/pdf/E8-20253.pdf> (consumer’s agreement with a seller to receive calls delivering prerecorded messages is nontransferable); *FTC, Complying with the Telemarketing Sales Rule, The Written Agreement Requirement*, <https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement>; but see, *Insurance Marketing Coalition, Ltd. v. Federal Communications Commission*, -- F.4th --, 2025 WL 289152 (11th Cir. 2025) (vacating and remanding FCC rule requiring those wishing to make a telemarketing or advertising robocall to obtain (1) consent from one called party to one seller at a time; and (2) consent that is logically and topically related to the interaction that prompted the consent).

²³ 47 U.S.C. § 227(e)(1); 47 C.F.R. § 64.1604.

²⁴ 47 U.S.C. § 227(e)(6).

²⁵ 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

²⁶ *Id.*

network. Voice service providers transmitting calls into and throughout the states are obligated to familiarize themselves with, and abide by, all applicable state laws.

Requested Action in Response to this Notice

As noted above, the Task Force is providing this Notice in order to memorialize some of its investigative findings to date. The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, and has been, accepted and transmitted by and through Lingo’s network, in order to ensure that your current business—and any subsequently-formed businesses—follow all applicable federal and state laws and regulations, including those referenced above. If subsequent investigation shows that Lingo and/or its principals continue to assist customers by initiating and/or transmitting call traffic not dissimilar from the traffic highlighted in this Notice, the Task Force may decide to pursue an enforcement action against Lingo, any later-formed business entities, and the principal owners and operators in common to both. Future action may also consist of referring the matter to the FCC for consideration of potential enforcement actions.²⁷

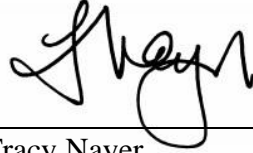
For your information, we have informed several of our federal law enforcement counterparts—including our colleagues at the FCC’s Enforcement Bureau—of the Task Force’s intention to issue this Notice to Lingo. Finally, this Notice does not waive or otherwise preclude the Task Force from bringing an enforcement action related to conduct preceding the date of this

²⁷ The FCC’s authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter, *see, e.g., FCC Orders Avid Telecom to Cease and Desist Robocalls* <https://www.fcc.gov/document/fcc-orders-avid-telecom-cess-and-desist-robocalls> (issued Jun. 7, 2023); *FCC Issues Robocall Cease-and-Desist Letter to PZ/Illum*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-pzillum> (issued Oct. 21, 2021), a K4 Public Notice, *see FCC Enforcement Bureau Notifies All U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting From One Eye LLC*, <https://www.fcc.gov/document/fcc-takes-repeat-robocall-offenders-attempts-evade-enforcement> (issued Feb. 15, 2023), a Notice of Apparent Liability, *see, e.g., John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948 (2020), *available at* https://docs.fcc.gov/public/attachments/FCC-20-74A1_Rcd.pdf, a Consumer Communications Information Services Threat (“C-CIST”) Designation Notice, *see FCC [Enforcement Bureau] Issues C-CIST Classification for “Royal Tiger”*, <https://www.fcc.gov/document/fcc-eb-issues-c-cist-classification-royal-tiger> (issued May 13, 2024), or proceedings that may result in removal from the Robocall Mitigation Database, *see, e.g., Viettel Business Solutions Company, Etihad Etisalat (Mobily), Claude ICT Poland Sp. z o. o. dba TeleCube.PL, Nervill LTD, Textodog Inc. dba Textodog and Textodog Software Inc., Phone GS, Computer Integrated Solutions dba CIS IT & Engineering, Datacom Specialists, DomainerSuite, Inc., Evernex SMC PVT LTD, Humbolt Voip, and My Taxi Ride Inc.*, Removal Order, 39 FCC Rcd 1319 (2024), *available at* <https://www.fcc.gov/document/fcc-removes-12-entities-robocall-mitigation-database>, the latter of which—if completed—would require all intermediate providers and terminating voice service providers to cease accepting your call traffic.

Notice, including conduct that resulted in violations related to the call traffic referenced in this Notice.

The Task Force remains steadfast in its resolve to meaningfully curb illegal robocall traffic. Please direct any inquiries regarding this Notice to my attention at tnayer@ncdoj.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "Tracy Nayer", written over a horizontal line.

Tracy Nayer
Special Deputy Attorney General
Consumer Protection Division
North Carolina Department of Justice

JEFF JACKSON
ATTORNEY GENERAL



TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL
TNAYER@NCDOJ.GOV

April 9, 2025

Chris Rubini, CEO
Range, Inc.
919 North Market Street, Suite 950
Wilmington, DE 19801
*Sent via certified mail, return receipt requested, and via email to chris@rangetelecom.com,
support@rangetelecom.com*

Re: SECOND AND FINAL NOTICE LETTER from the Anti-Robocall Multistate Litigation Task Force Concerning Range, Inc.'s Involvement in Suspected Illegal Robocall Traffic

Dear Mr. Rubini:

The Anti-Robocall Multistate Litigation Task Force's ("Task Force")¹ investigation of Range, Inc. ("Range")² has shown that Range has transmitted suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is the Task Force's second and final attempt to informally apprise you of the Task Force's concerns regarding Range call traffic, and to caution Range that it should scrutinize the call traffic of its current customers, evaluate the efficacy of its existing robocall mitigation policies, and cease transmitting illegal traffic on behalf of its current customers.

The Task Force provides this Notice in order to memorialize some of its investigative findings to date.

¹ The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall ecosystem that are identified as being responsible for significant volumes of illegal and fraudulent robocall traffic routed into and across the country.

² Range, Inc.—FCC Registration No. 0026012666; Robocall Mitigation Database No. RMD0001995—"Range") is a Delaware corporation. Chris Rubini serves as Range's Chief Executive Officer. Vince Tozzi is Range's President, and Sam Jones is Chief Technology Officer. The FCC's Robocall Mitigation Database indicates that Wrazzle, Inc. is an affiliate, subsidiary, or parent company of Range. Wrazzle, Inc. FCC Registration No. 32836934; Robocall Mitigation Database No. RMD0012545—"Range") is a Connecticut corporation, for which Chris Rubini also serves as CEO.

Task Force’s Findings Regarding Range’s Call Traffic

As you are aware, on August 1, 2022, the Task Force issued its Civil Investigative Demand (“CID”) to Range to identify, investigate, and mitigate suspected illegal call traffic that is or was accepted onto, and transmitted across, Range’s network. On November 3, 2023, the Task Force issued a Notice to Range (“2023 Task Force Notice”) memorializing some of the Task Force’s findings concerning Range’s call traffic, informing you of the Task Force’s concerns regarding your call traffic, and cautioning Range that it should cease transmitting any illegal traffic immediately. Based on pertinent analyses and information available to the Task Force, it appears that Range transmitted calls associated with high-volume illegal and/or suspicious robocall campaigns.

During the course of its investigation of Range, the Task Force requested the production of call detail records for all call traffic sent to and/or through your network or which you originated on behalf of your customers during a certain time period. Additionally, as noted in the 2023 Task Force Notice, as part of its investigation into the transmission of illegal robocalls and the providers and entities that originate and/or route them, the Task Force regularly reviews call traffic information from several industry sources, including USTelecom’s Industry Traceback Group (“ITG”).³

Call traffic data from the ITG shows that it issued at least **592 traceback notices** to Range since January 2019 for calls it accepted and/or transmitted onto and across the U.S. telephone network. These notices from the ITG cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning government imposters and impersonations, utilities rebates, Amazon, Medicare advisor, financial impersonations and credit card interest rate reductions, auto warranties and others, with Range identified as serving in various roles in the call path. At least **242 traceback notices** were issued since August 2022, when the Task Force issued its first CID to Range. While the traceback notices issued since August 2022 show that Range is no longer identified as the point-of-entry or gateway⁴ provider for this traffic, there is still a portion of this traffic for which Range is identified as the immediate downstream provider to the originating

³ Established in 2015, the ITG is a private collaborative industry group—composed of providers across wireline, wireless, VOIP, and cable services—that traces and identifies the sources of suspected illegal and suspicious robocalls. In December 2019, Congress enacted the Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) to combat the scourge of unlawful robocalls. *See* Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019). Following its enactment, the Federal Communications Commission designated the ITG as the official private-led traceback consortium charged with leading the voice communications industry’s efforts to trace the origin of suspected illegal robocalls through various communications networks through tracebacks. *See* 47 C.F.R. § 64.1203.

⁴ *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, 87 FR 42916, 42917–18, para. 7 (2022) (defining a “gateway provider” as “a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider”).

provider. Because the ITG estimates that each traced call is representative of a large volume of similar illegal and/or suspicious calls,⁵ Range likely continued to cause significant volumes of illegal and/or suspicious robocalls to ultimately reach U.S. consumers, despite traceback notifications from the ITG of this identified and suspected illegal call traffic.

Further, an analysis of a set of call detail records⁶ from Range’s nationwide call traffic between March 2021 and September 2022 shows that more than **409.6 million calls were made using invalid Caller ID numbers**, which means the calling numbers making the calls used a combination of numbers that were not assigned and/or recognized as valid by the North American Numbering Plan Administrator. Each call made using an invalid calling telephone number appears to have violated the Truth in Caller ID, 47 U.S.C. 227(e)(1) and 47 C.F.R. 64.1604(a), and the TCPA, 47 C.F.R. § 64.1200(n)(4)–(5).

Additionally, Range’s nationwide call traffic included more than **3.29 million calls using illegally spoofed telephone numbers** for this same time period. The illegally spoofed calling numbers disguised calls as legitimate call traffic from local, state, and federal government agencies within the United States, and misrepresented callers’ affiliations with law enforcement agencies and private sector entities. Each call made using an illegally spoofed calling telephone number appears to have violated the TSR, 16 C.F.R. § 310.4(a)(8), and the Truth in Caller ID: 47 U.S.C. § 227(e)(1) and 47 C.F.R. § 64.1604(a).

Finally, after an analysis of a subset of recorded voicemail messages that corresponded with the call detail records, more than **464,000 calls contained unlawful or fraudulent content**,

⁵ USTelecom, *Industry Traceback Group Policies and Procedures*, at 4 (last revised April 2022) (*ITG Policies & Procedures*) (defining “campaign” as “[a] group of calls with identical or nearly identical messaging as determined by the content and calling patterns of the caller,” where “[a] single Campaign often represents hundreds of thousands or millions of calls”), *available at* <https://r01986.a2cdn1.secureserver.net/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf>.

⁶ Call detail records or “CDRs” are automatically generated records of each attempted or completed call that reaches and/or crosses a voice service provider’s network. CDRs generally include the following information:

- a. The date and time of the call attempt;
- b. The duration of the call (calls that fail to connect are generally denoted by a zero-second duration);
- c. The intended call recipient’s telephone number;
- d. The originating or calling number from which the call was placed (which may be a real number or may be spoofed);
- e. An identifier such as a name or account number for the upstream provider that sent the call attempt to the provider’s network; and
- f. An identifier for the downstream provider to which the provider attempts to route the call.

with each call's content appearing to have violated the TSR, 16 C.F.R. § 310.3(a)(2)(iii), and/or the TCPA, 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B), 47 C.F.R. § 64.1200(a)(2)–(3).

Lastly, analysis of a portion of Range's likely involvement in the routing of nationwide call traffic concerning Amazon/Apple imposter robocalls was assessed. Between September 2021 and August 2022, among a nationwide sample of over 1.12 million transcribed and recorded Amazon/Apple imposter robocalls, **approximately 76,300 of these Amazon/Apple imposter robocalls are estimated to be attributable to Range.** Thus, of the more than 563 million estimated Amazon/Apple imposter robocalls reaching consumers across the country in this sample during this period, **approximately 38 million of these scam robocalls are estimated to be attributable to Range.**

A similar and more recent analysis of Range's likely involvement in the routing of nationwide call traffic concerning this same government imposter scam was also assessed. During the three-month period between October 2024 and December 2024, among a nationwide sample of 222,799 transcribed and recorded SSA imposter robocalls, **approximately 27,438 of these SSA imposter robocalls are estimated to be attributable to Range.** Thus, of the over 111 million estimated SSA imposter robocalls reaching consumers across the country in this sample during this limited period, **approximately 13.7 million of these scam robocalls are estimated to be attributable to Range.**

After reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force has concluded that Range is and/or has been involved in, at a minimum, transmitting call traffic indicative of, and associated with, recurrent high-volume illegal and/or suspicious robocalling campaigns and/or practices, which conduct could subject Range to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and state laws.

Overview of Select Relevant Laws

As Range well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,⁷ the Telephone Consumer Protection Act,⁸ and/or the Truth in Caller ID Act,⁹ as well as state consumer protection statutes.

Telemarketing Sales Rule (15 U.S.C. §§ 6101–6108; 16 C.F.R. Part 310)

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act which directed the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices.¹⁰ Pursuant to this directive, the FTC promulgated the Telemarketing Sales Rule (“TSR”). It is a violation of the TSR for voice service providers to provide substantial assistance

⁷ 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4.

⁸ 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

⁹ 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

¹⁰ 15 U.S.C. § 6102.

to customers that the provider “knows or consciously avoids knowing” are engaged in practices that violate TSR provisions against deceptive and abusive telemarketing acts or practices.¹¹ State Attorneys General have concurrent authority with the FTC to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR.¹²

Telephone Consumer Protection Act (47 U.S.C. § 227; 47 C.F.R. §§ 64.1200 and 64.1604)

Under the Telephone Consumer Protection Act (“TCPA”), the FCC promulgated rules restricting calls made with automated telephone dialing systems and calls delivering artificial or prerecorded voice messages.¹³ Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.¹⁴ State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.¹⁵ The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,¹⁶ including those made with the “prior express consent” of the called party or with “prior express *written* consent” of the called party for telemarketing calls.¹⁷ Note, however, the FCC has found in at least one instance that single consents purportedly given by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.¹⁸

¹¹ 16 C.F.R. § 310.3(b).

¹² 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

¹³ 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3).

¹⁴ 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2).

¹⁵ 47 U.S.C. § 227(g)(1).

¹⁶ 47 U.S.C. § 227(b)(1)(A)–(B), (b)(2)(B); 47 C.F.R. § 64.1200(a)(1)–(3), (a)(9).

¹⁷ 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

¹⁸ For example, in November 2022, the FCC issued an order requiring all voice service providers to block calls from provider Urth Access, LLC. In response to allegations concerning the transmission of illegal robocalls, Urth Access claimed to have obtained express consent for each of the calls. However, that consent stemmed from websites where consumers purportedly agreed to receive robocalls from over 5,000 “marketing partners” listed on a separate site. The FCC found this type of practice insufficient to constitute express consent to the marketing partners to contact the consumers. See *FCC Orders Voice Service Providers to Block Student Loan Robocalls*, <https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls> (Order); *FCC Issues Robocall Cease-and-Desist Letter to Urth Access*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-urth-access> (Cease-and-Desist Letter). We note that this decision is consistent with the FTC’s interpretation of the express consent requirement of the TSR. See Federal Register, Vol. 73 No. 169, 2008 at 51182, <https://www.govinfo.gov/content/pkg/FR-2008-08-29/pdf/E8-20253.pdf> (consumer’s agreement with a seller to receive calls delivering prerecorded messages is nontransferable); *FTC, Complying with the Telemarketing Sales Rule, The Written Agreement Requirement*, <https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales->

Truth in Caller ID Act (47 U.S.C. § 227(e))

Under the federal Truth in Caller ID Act, it is generally unlawful for a person to “knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.”¹⁹ State Attorneys General have the authority to bring enforcement actions for violations of the Truth in Caller ID Act and its prohibition against illegal caller identification spoofing.²⁰ Such violative conduct can lead to assessments of civil penalties of up to \$10,000 for each violation, or three times that amount for each day of continuing violations.²¹ Note that any penalties for violations of the Truth in Caller ID Act are in addition to those assessed for any other penalties provided for by the TCPA.²²

General Note regarding State Laws

In addition to their authority to enforce the above federal statutes, State Attorneys General are empowered to enforce their respective state laws regulating various aspects of the initiation and transmission of illegal robocall and telemarketing call traffic across the U.S. telephone network. Voice service providers transmitting calls into and throughout the states are obligated to familiarize themselves with, and abide by, all applicable state laws.

Requested Action in Response to this Notice

As noted above, the Task Force is providing this Notice in order to memorialize some of its investigative findings to date. The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, and has been, accepted and transmitted by and through Range’s network, in order to ensure that your current business—and any subsequently-formed businesses—follow all applicable federal and state laws and regulations, including those referenced above. If subsequent investigation shows that Range and/or its principals assist customers by initiating and/or transmitting call traffic not dissimilar from the traffic highlighted in this Notice, the Task Force may decide to pursue an enforcement action against Range, any later-formed business entities, and the principal owners and

[rule#writtenagreement](#); but see, *Insurance Marketing Coalition, Ltd. v. Federal Communications Commission*, -- F.4th --, 2025 WL 289152 (11th Cir. 2025) (vacating and remanding FCC rule requiring those wishing to make a telemarketing or advertising robocall to obtain (1) consent from one called party to one seller at a time; and (2) consent that is logically and topically related to the interaction that prompted the consent).

¹⁹ 47 U.S.C. § 227(e)(1); 47 C.F.R. § 64.1604.

²⁰ 47 U.S.C. § 227(e)(6).

²¹ 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

²² *Id.*

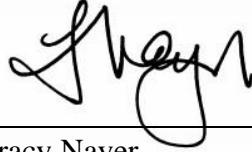
operators in common to both. Future action may also consist of referring the matter to the FCC for consideration of potential enforcement actions.²³

For your information, we have informed several of our federal law enforcement counterparts—including our colleagues at the FCC’s Enforcement Bureau—of the Task Force’s intention to issue this Notice to Range. Finally, this Notice does not waive or otherwise preclude the Task Force from bringing an enforcement action related to conduct preceding the date of this Notice, including conduct that resulted in violations related to the call traffic referenced in this Notice.

²³ The FCC’s authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter, *see, e.g., FCC Orders Avid Telecom to Cease and Desist Robocalls* <https://www.fcc.gov/document/fcc-orders-avid-telecom-cess-and-desist-robocalls> (issued Jun. 7, 2023); *FCC Issues Robocall Cease-and-Desist Letter to PZ/Illum*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-pzillum> (issued Oct. 21, 2021), a K4 Public Notice, *see FCC Enforcement Bureau Notifies All U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting From One Eye LLC*, <https://www.fcc.gov/document/fcc-takes-repeat-robocall-offenders-attempts-evade-enforcement> (issued Feb. 15, 2023), a Notice of Apparent Liability, *see, e.g., John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948 (2020), *available at* https://docs.fcc.gov/public/attachments/FCC-20-74A1_Rcd.pdf, a Consumer Communications Information Services Threat (“C-CIST”) Designation Notice, *see FCC [Enforcement Bureau] Issues C-CIST Classification for “Royal Tiger”*, <https://www.fcc.gov/document/fcc-eb-issues-c-cist-classification-royal-tiger> (issued May 13, 2024), or proceedings that may result in removal from the Robocall Mitigation Database, *see, e.g., Viettel Business Solutions Company, Etihad Etisalat (Mobily), Claude ICT Poland Sp. z o. o. dba TeleCube.PL, Nervill LTD, Textodog Inc. dba Textodog and Textodog Software Inc., Phone GS, Computer Integrated Solutions dba CIS IT & Engineering, Datacom Specialists, DomainerSuite, Inc., Evernex SMC PVT LTD, Humbolt Voip, and My Taxi Ride Inc.*, Removal Order, 39 FCC Rcd 1319 (2024), *available at* <https://www.fcc.gov/document/fcc-removes-12-entities-robocall-mitigation-database>, the latter of which—if completed—would require all intermediate providers and terminating voice service providers to cease accepting your call traffic.

The Task Force remains steadfast in its resolve to meaningfully curb illegal robocall traffic. Please direct any inquiries regarding this Notice to my attention at tnayer@ncdoj.gov.

Sincerely,

A handwritten signature in black ink, appearing to read 'Tracy Nayer', written over a horizontal line.

Tracy Nayer
Special Deputy Attorney General
Consumer Protection Division
North Carolina Department of Justice

JEFF JACKSON
ATTORNEY GENERAL



TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL
TNAYER@NCDOJ.GOV

April 9, 2025

Talal Khalid, CEO
Telcast Network, LLC
c/o Thomas M. Lynch, Esq.
Thomas Lynch & Associates
6 Carrolls Tract Road, No. 506
Fairfield, PA 17320

Sent via certified mail, return receipt requested, and via email to tlynch@telecomlawyers.com

Re: SECOND AND FINAL NOTICE LETTER from the Anti-Robocall Multistate Litigation Task Force Concerning Telcast Network, LLC's Continued Involvement in Suspected Illegal Robocall Traffic

Dear Mr. Khalid:

The Anti-Robocall Multistate Litigation Task Force's ("Task Force")¹ investigation of Telcast Network, LLC ("Telcast")² has shown that Telcast has transmitted, and continues to transmit, suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is the Task Force's second and final attempt to informally apprise you of the Task Force's concerns regarding Telcast call traffic, and to caution Telcast that it should scrutinize the call traffic of its current customers, evaluate the efficacy of its existing robocall mitigation policies, and cease transmitting illegal traffic on behalf of its current customers.

The Task Force provides this Notice in order to memorialize some of its investigative findings to date.

¹ The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall ecosystem that are identified as being responsible for significant volumes of illegal and fraudulent robocall traffic routed into and across the country.

² Telcast Network, LLC—FCC Registration No. 0026902635; Robocall Mitigation Database No. RMD0001732—"Telcast") provides an Atlanta, Georgia business address in the FCC's Robocall Mitigation Database. Talal Khalid is identified as Telcast's Chief Executive Officer. Babar Ahmed is Telcast's Chief Operating Officer.

Task Force’s Findings Regarding Telcast’s Call Traffic

As you are aware, on August 1, 2022, the Task Force issued its Civil Investigative Demand (“CID”) to Telcast to identify, investigate, and mitigate suspected illegal call traffic that is or was accepted onto, and transmitted across, Telcast’s network.

On March 17, 2023, Telcast was issued a Cease-and-Desist Demand³ from the Federal Trade Commission (“FTC”). The FTC’s Cease-and-Desist provided that Telcast was knowingly routing and transmitting illegal robocall traffic identified therein.⁴ The FTC’s Cease-and-Desist referenced applicable federal laws and rules, and Telcast’s legal obligations under the same.

On November 3, 2023, the Task Force issued a Notice to Telcast (“2023 Task Force Notice”) memorializing some of the Task Force’s findings concerning Telcast’s call traffic, informing you of the Task Force’s continuing concerns regarding your call traffic, and cautioning Telcast that it should cease transmitting any illegal traffic immediately. Based on pertinent analyses and information available to the Task Force, it appears that Telcast has continued to transmit calls associated with high-volume illegal and/or suspicious robocall campaigns.

As noted in the 2023 Task Force Notice, as part of its investigation into the transmission of illegal robocalls and the providers and entities that originate and/or route them, the Task Force regularly reviews call traffic information from several industry sources, including USTelecom’s Industry Traceback Group (“ITG”)⁵ and ZipDX LLC (“ZipDX”)⁶.

³ FTC, *Cease and Desist Demand to Telcast Network LLC*, https://www.ftc.gov/system/files/ftc_gov/pdf/pointofnoentry-telcastnetworkceasedesistletterfinaljms.pdf (hereinafter “FTC’s Cease-and-Desist”).

⁴ FTC’s Cease-and-Desist at 1–2.

⁵ Established in 2015, the ITG is a private collaborative industry group—composed of providers across wireline, wireless, VOIP, and cable services—that traces and identifies the sources of suspected illegal and suspicious robocalls. In December 2019, Congress enacted the Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) to combat the scourge of unlawful robocalls. *See* Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019). Following its enactment, the Federal Communications Commission designated the ITG as the official private-led traceback consortium charged with leading the voice communications industry’s efforts to trace the origin of suspected illegal robocalls through various communications networks through tracebacks. *See* 47 C.F.R. § 64.1203.

⁶ ZipDX is a provider of web- and phone-based collaboration services, which also focuses resources on developing and making technology available that is directed at mitigating illegal robocalls and other telephone-based fraud and abuse. ZipDX’s proprietary tool “RRAPTOR” is one such technology, which is an automated robocall surveillance tool that captures call recordings and information for calls largely associated with high-volume suspicious calling campaigns, and identifies the providers who have affixed their SHAKEN signatures to each of the captured calls, indicating that the provider is in the call path and whether those providers have attested to knowing

Call traffic data from the ITG shows that it issued at least **800 traceback notices** to Telcast since January 2019 for calls it accepted and/or transmitted onto and across the U.S. telephone network. These notices from the ITG cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning financial and utility impersonations, utilities rebate, Medicare advisor, Amazon, tax relief, and others, with Telcast identified as serving in various roles in the call path. At least **517 traceback notices** were issued since August 2022—after the Task Force issued its CID to Telcast—and, of those, still more than **174 traceback notices** were issued since the 2023 Task Force Notice. While the traceback notices issued since August 2022 show that Telcast is no longer identified as the point-of-entry or gateway⁷ provider for this traffic, there is still a portion of this traffic for which Telcast is identified as the immediate downstream provider to the originating provider. Because the ITG estimates that each traced call is representative of a large volume of similar illegal and/or suspicious calls,⁸ Telcast is likely continuing to cause significant volumes of illegal and/or suspicious robocalls to ultimately reach U.S. consumers, despite traceback notifications from the ITG of this identified and suspected illegal call traffic.

Information available from ZipDX indicates that Telcast also attested to calls for a number of the same high-volume robocalling campaigns for which it received and/or continues to receive traceback notices from the ITG. For instance, during the last year, ZipDX identified **7,394 suspicious calls** transmitted by Telcast **from 7,331 unique calling numbers**,⁹ exhibiting characteristics indicative of calls that are violations of federal and state laws; 87% of these calls

the calling party who made the suspicious call and/or knowing of the calling party’s right to use that calling number to make that suspicious call. See ZipDX, What is RRAPTOR?, <https://legalcallsonly.org/what-is-rraptor/> (last visited Oct. 17, 2024).

⁷ *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, 87 FR 42916, 42917–18, para. 7 (2022) (defining a “gateway provider” as “a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider”).

⁸ USTelecom, *Industry Traceback Group Policies and Procedures*, at 4 (last revised April 2022) (*ITG Policies & Procedures*) (defining “campaign” as “[a] group of calls with identical or nearly identical messaging as determined by the content and calling patterns of the caller,” where “[a] single Campaign often represents hundreds of thousands or millions of calls”), available at <https://r01986.a2cdn1.secureserver.net/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf>.

⁹ The use of many unique calling numbers for this volume of called numbers indicates a suspicious pattern in your call traffic of “snowshoeing” or “snowshoe spoofing,” which is a practice often employed by illegal robocallers and telemarketers to circumvent the protections of the STIR/SHAKEN call authentication framework by using significant quantities of unique numbers for caller IDs on a short-term or rotating basis in order to evade behavioral analytics detection, or to bypass or hinder call blocking or call labeling analytics based on the origination numbers. Telephone numbers used for snowshoeing sometimes cannot themselves receive incoming calls, which has the effect of impeding an audit of the legitimacy of these calling numbers.

were also made to numbers that have been registered on the National Do Not Call Registry.¹⁰ Further, more than 99% of these calls were signed by Telcast with a C-Level STIR/SHAKEN attestation, indicating that Telcast received the call without a signature. While we recognize Telcast's obligation as an intermediate provider to affix an attestation to every unsigned call that it receives, we are concerned that your upstream call source(s) are continuing to fail to affix an A- or B-attested signature of their own, and that your acceptance of these calls despite that failure is evidence of Telcast's culpability for these calls. Given the prolific nature of the calls, the Task Force is concerned about whether Telcast is still failing to take any proactive steps to mitigate this traffic.

Lastly, analysis of a portion of Telcast's likely involvement in the routing of nationwide call traffic concerning utility scams was assessed. Between March 2021 and March 2022, among a nationwide sample of over 1.85 million transcribed and recorded utility scam robocalls, **more than 596,400 of these utility scam robocalls are estimated to be attributable to Telcast.** Thus, of the more than 927.6 million utility scam robocalls reaching consumers across the country in this sample between March 2021 and March 2022, **more than 298.2 million of these scam robocalls are estimated to be attributable to Telcast.**

After reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force has concluded that Telcast is and/or has been involved in, at a minimum, transmitting call traffic indicative of, and associated with, recurrent high-volume illegal and/or suspicious robocalling campaigns and/or practices, which conduct could subject Telcast to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and state laws.

Overview of Select Relevant Laws

As Telcast well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,¹¹ the Telephone Consumer Protection Act,¹² and/or the Truth in Caller ID Act,¹³ as well as state consumer protection statutes.

Telemarketing Sales Rule (15 U.S.C. §§ 6101–6108; 16 C.F.R. Part 310)

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act which directed the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices.¹⁴ Pursuant to this directive, the FTC promulgated the Telemarketing Sales Rule ("TSR"). It is a violation of the TSR for voice service providers to provide substantial assistance to customers that the provider "knows or consciously avoids knowing" are engaged in practices

¹⁰ Most calls captured by RRAPTOR are calls made to phone numbers that have been registered on the National Do Not Call Registry.

¹¹ 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4.

¹² 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

¹³ 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

¹⁴ 15 U.S.C. § 6102.

that violate TSR provisions against deceptive and abusive telemarketing acts or practices.¹⁵ State Attorneys General have concurrent authority with the FTC to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR.¹⁶

Telephone Consumer Protection Act (47 U.S.C. § 227; 47 C.F.R. §§ 64.1200 and 64.1604)

Under the Telephone Consumer Protection Act (“TCPA”), the FCC promulgated rules restricting calls made with automated telephone dialing systems and calls delivering artificial or prerecorded voice messages.¹⁷ Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.¹⁸ State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.¹⁹ The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,²⁰ including those made with the “prior express consent” of the called party or with “prior express *written* consent” of the called party for telemarketing calls.²¹ Note, however, the FCC has found in at least one instance that single consents purportedly given by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.²²

¹⁵ 16 C.F.R. § 310.3(b).

¹⁶ 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

¹⁷ 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3).

¹⁸ 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2).

¹⁹ 47 U.S.C. § 227(g)(1).

²⁰ 47 U.S.C. § 227(b)(1)(A)–(B), (b)(2)(B); 47 C.F.R. § 64.1200(a)(1)–(3), (a)(9).

²¹ 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

²² For example, in November 2022, the FCC issued an order requiring all voice service providers to block calls from provider Urth Access, LLC. In response to allegations concerning the transmission of illegal robocalls, Urth Access claimed to have obtained express consent for each of the calls. However, that consent stemmed from websites where consumers purportedly agreed to receive robocalls from over 5,000 “marketing partners” listed on a separate site. The FCC found this type of practice insufficient to constitute express consent to the marketing partners to contact the consumers. See *FCC Orders Voice Service Providers to Block Student Loan Robocalls*, <https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls> (Order); *FCC Issues Robocall Cease-and-Desist Letter to Urth Access*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-urth-access> (Cease-and-Desist Letter). We note that this decision is consistent with the FTC’s interpretation of the express consent requirement of the TSR. See Federal Register, Vol. 73 No. 169, 2008 at 51182, <https://www.govinfo.gov/content/pkg/FR-2008-08-29/pdf/E8-20253.pdf> (consumer’s agreement with a seller to receive calls delivering prerecorded messages is nontransferable); *FTC, Complying with the Telemarketing Sales Rule, The Written Agreement Requirement*, <https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement>; but see, *Insurance Marketing Coalition, Ltd. v. Federal Communications*

Truth in Caller ID Act (47 U.S.C. § 227(e))

Under the federal Truth in Caller ID Act, it is generally unlawful for a person to “knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.”²³ State Attorneys General have the authority to bring enforcement actions for violations of the Truth in Caller ID Act and its prohibition against illegal caller identification spoofing.²⁴ Such violative conduct can lead to assessments of civil penalties of up to \$10,000 for each violation, or three times that amount for each day of continuing violations.²⁵ Note that any penalties for violations of the Truth in Caller ID Act are in addition to those assessed for any other penalties provided for by the TCPA.²⁶

General Note regarding State Laws

In addition to their authority to enforce the above federal statutes, State Attorneys General are empowered to enforce their respective state laws regulating various aspects of the initiation and transmission of illegal robocall and telemarketing call traffic across the U.S. telephone network. Voice service providers transmitting calls into and throughout the states are obligated to familiarize themselves with, and abide by, all applicable state laws.

Requested Action in Response to this Notice

As noted above, the Task Force is providing this Notice in order to memorialize some of its investigative findings to date. The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, and has been, accepted and transmitted by and through Telcast’s network, in order to ensure that your current business—and any subsequently-formed businesses—follow all applicable federal and state laws and regulations, including those referenced above. If subsequent investigation shows that Telcast and/or its principals continue to assist customers by initiating and/or transmitting call traffic not dissimilar from the traffic highlighted in this Notice, the Task Force may decide to pursue an enforcement action against Telcast, any later-formed business entities, and the principal owners and operators in common to both. Future action may also consist of referring the matter to the FCC for consideration of potential enforcement actions.²⁷

Commission, -- F.4th --, 2025 WL 289152 (11th Cir. 2025) (vacating and remanding FCC rule requiring those wishing to make a telemarketing or advertising robocall to obtain (1) consent from one called party to one seller at a time; and (2) consent that is logically and topically related to the interaction that prompted the consent).

²³ 47 U.S.C. § 227(e)(1); 47 C.F.R. § 64.1604.

²⁴ 47 U.S.C. § 227(e)(6).

²⁵ 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

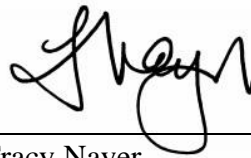
²⁶ *Id.*

²⁷ The FCC’s authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter, *see, e.g., FCC Orders Avid Telecom to Cease and Desist*

For your information, we have informed several of our federal law enforcement counterparts—including our colleagues at the FCC’s Enforcement Bureau—of the Task Force’s intention to issue this Notice to Telcast. Finally, this Notice does not waive or otherwise preclude the Task Force from bringing an enforcement action related to conduct preceding the date of this Notice, including conduct that resulted in violations related to the call traffic referenced in this Notice.

The Task Force remains steadfast in its resolve to meaningfully curb illegal robocall traffic. Please direct any inquiries regarding this Notice to my attention at tnayer@ncdoj.gov.

Sincerely,



Tracy Nayer
Special Deputy Attorney General
Consumer Protection Division
North Carolina Department of Justice

Robocalls <https://www.fcc.gov/document/fcc-orders-avid-telecom-cess-and-desist-robocalls> (issued Jun. 7, 2023); *FCC Issues Robocall Cease-and-Desist Letter to PZ/Illum*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-pzillum> (issued Oct. 21, 2021), a K4 Public Notice, *see FCC Enforcement Bureau Notifies All U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting From One Eye LLC*, <https://www.fcc.gov/document/fcc-takes-repeat-robocall-offenders-attempts-evade-enforcement> (issued Feb. 15, 2023), a Notice of Apparent Liability, *see, e.g., John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948 (2020), *available at* https://docs.fcc.gov/public/attachments/FCC-20-74A1_Rcd.pdf, a Consumer Communications Information Services Threat (“C-CIST”) Designation Notice, *see FCC [Enforcement Bureau] Issues C-CIST Classification for “Royal Tiger”*, <https://www.fcc.gov/document/fcc-eb-issues-c-cist-classification-royal-tiger> (issued May 13, 2024), or proceedings that may result in removal from the Robocall Mitigation Database, *see, e.g., Viettel Business Solutions Company, Etihad Etisalat (Mobily), Claude ICT Poland Sp. z o. o. dba TeleCube.PL, Nervill LTD, Textodog Inc. dba Textodog and Textodog Software Inc., Phone GS, Computer Integrated Solutions dba CIS IT & Engineering, Datacom Specialists, DomainerSuite, Inc., Evernex SMC PVT LTD, Humbolt Voip, and My Taxi Ride Inc.*, Removal Order, 39 FCC Rcd 1319 (2024), *available at* <https://www.fcc.gov/document/fcc-removes-12-entities-robocall-mitigation-database>, the latter of which—if completed—would require all intermediate providers and terminating voice service providers to cease accepting your call traffic.

JEFF JACKSON
ATTORNEY GENERAL



TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL
TNAYER@NCDOJ.GOV

April 9, 2025

Lamar Carter, CEO
All Access Telecom, Inc.
771 East US Hwy 80, Suite 201
Forney, Texas 75216

Sent via certified mail, return receipt requested, and via email to
lamar.carter@allaccesstelecom.com, martin.potia@allaccesstelecom.com,
jorge.ramos@allaccesstelecom.com, marla.riebock@allaccesstelecom.com,
cathy@allaccesstelecom.com

Re: SECOND AND FINAL NOTICE LETTER from the Anti-Robocall Multistate Litigation Task Force Concerning All Access Telecom, Inc.'s Continued Involvement in Suspected Illegal Robocall Traffic

Dear Mr. Carter:

The Anti-Robocall Multistate Litigation Task Force's ("Task Force")¹ investigation of All Access Telecom, Inc. ("All Access")² has shown that All Access has transmitted, and continues to transmit, suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is the Task Force's second and final attempt to informally apprise you of the Task Force's concerns regarding All Access' call traffic, and to caution All Access that it should scrutinize the call traffic of its current customers, evaluate the efficacy of its existing robocall mitigation policies, and cease transmitting illegal traffic on behalf of its current customers.

The Task Force provides this Notice in order to memorialize some of its investigative findings to date.

¹ The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall ecosystem that are identified as being responsible for significant volumes of illegal and fraudulent robocall traffic routed into and across the country.

² All Access Telecom, Inc.—FCC Registration No. 0019397843; Robocall Mitigation Database No. RMD0017654—"All Access") is a Texas corporation. Lamar Carter serves as All Access's Chief Executive Officer. Martin Potia is Chief Operations Officer, Jorge Ramos is Chief Technology Officer, Marla Riebock is Director of Carrier Relations, and Cathy Dodson is Finance Director.

Task Force’s Findings Regarding All Access’s Call Traffic

As you are aware, on August 1, 2022, the Task Force issued its Civil Investigative Demand (“CID”) to All Access to identify, investigate, and mitigate suspected illegal call traffic that is accepted onto, and transmitted across, All Access’s network. On November 3, 2023, the Task Force issued a Notice to All Access (“2023 Task Force Notice”) memorializing some of the Task Force’s findings concerning All Access’s call traffic, informing you of the Task Force’s continuing concerns regarding your call traffic, and cautioning All Access that it should cease transmitting any illegal traffic immediately. Based on pertinent analyses and information available to the Task Force, it appears that All Access has continued to transmit calls associated with high-volume illegal and/or suspicious robocall campaigns.

During the course of its investigation of All Access, the Task Force requested the production of call detail records for all call traffic sent to and/or through your network or which you originated on behalf of your customers during a certain time period. Additionally, as noted in the 2023 Task Force Notice, as part of its investigation into the transmission of illegal robocalls and the providers and entities that originate and/or route them, the Task Force regularly reviews call traffic information from several industry sources, including USTelecom’s Industry Traceback Group (“ITG”)³ and ZipDX LLC (“ZipDX”).⁴

Call traffic data from the ITG shows that it issued at least **1,630 traceback notices** to All Access since at or before January 2019 for calls it accepted and/or transmitted onto and across the U.S. telephone network. These notices from the ITG cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning government and financial imposters and impersonations, Amazon suspicious charges, credit card “courtesy” calls, credit card interest rate reductions, Medicare scams, political impersonations, cable discount scams, and others, with All

³ Established in 2015, the ITG is a private collaborative industry group—composed of providers across wireline, wireless, VOIP, and cable services—that traces and identifies the sources of suspected illegal and suspicious robocalls. In December 2019, Congress enacted the Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) to combat the scourge of unlawful robocalls. *See* Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019). Following its enactment, the Federal Communications Commission designated the ITG as the official private-led traceback consortium charged with leading the voice communications industry’s efforts to trace the origin of suspected illegal robocalls through various communications networks through tracebacks. *See* 47 C.F.R. § 64.1203.

⁴ ZipDX is a provider of web- and phone-based collaboration services, which also focuses resources on developing and making technology available that is directed at mitigating illegal robocalls and other telephone-based fraud and abuse. ZipDX’s proprietary tool “RRAPTOR” is one such technology, which is an automated robocall surveillance tool that captures call recordings and information for calls largely associated with high-volume suspicious calling campaigns, and identifies the providers who have affixed their SHAKEN signatures to each of the captured calls, indicating that the provider is in the call path and whether those providers have attested to knowing the calling party who made the suspicious call and/or knowing of the calling party’s right to use that calling number to make that suspicious call. *See* ZipDX, What is RRAPTOR?, <https://legalcallsonly.org/what-is-rraptor/> (last visited Oct. 17, 2024).

Access identified as serving in various roles in the call path. At least **720 traceback notices** were issued since August 2022—after the Task Force issued its CID to All Access—and, of those, still more than **356 traceback notices** were issued since the 2023 Task Force Notice. While the traceback notices issued since August 2022 show that All Access is not being identified as the point-of-entry or gateway⁵ provider for this traffic, there is still a portion of this traffic for which All Access is identified as the immediate downstream provider to the originating provider. Because the ITG estimates that each traced call is representative of a large volume of similar illegal and/or suspicious calls,⁶ All Access is likely continuing to cause significant volumes of illegal and/or suspicious robocalls to ultimately reach U.S. consumers, despite traceback notifications from the ITG of this identified and suspected illegal call traffic.

Further, an analysis of a limited set of call detail records⁷ from All Access’s nationwide call traffic for a period of less than three months between mid-July 2022 and the beginning of October 2022 shows that more than **730.7 million calls were made using invalid Caller ID numbers**, which means the calling numbers making the calls used a combination of numbers that were not assigned and/or recognized as valid by the North American Numbering Plan Administrator. Each call made using an invalid calling telephone number appears to have violated

⁵ *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, 87 FR 42916, 42917–18, para. 7 (2022) (defining a “gateway provider” as “a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider”).

⁶ USTelecom, *Industry Traceback Group Policies and Procedures*, at 4 (last revised April 2022) (*ITG Policies & Procedures*) (defining “campaign” as “[a] group of calls with identical or nearly identical messaging as determined by the content and calling patterns of the caller,” where “[a] single Campaign often represents hundreds of thousands or millions of calls”), available at <https://r01986.a2cdn1.secureserver.net/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf>.

⁷ Call detail records or “CDRs” are automatically generated records of each attempted or completed call that reaches and/or crosses a voice service provider’s network. CDRs generally include the following information:

- a. The date and time of the call attempt;
- b. The duration of the call (calls that fail to connect are generally denoted by a zero-second duration);
- c. The intended call recipient’s telephone number;
- d. The originating or calling number from which the call was placed (which may be a real number or may be spoofed);
- e. An identifier such as a name or account number for the upstream provider that sent the call attempt to the provider’s network; and
- f. An identifier for the downstream provider to which the provider attempts to route the call.

the Truth in Caller ID, 47 U.S.C. 227(e)(1) and 47 C.F.R. 64.1604(a), and the TCPA, 47 C.F.R. § 64.1200(n)(4)–(5).

Additionally, All Access’s nationwide call traffic included more than **4.39 million calls using illegally spoofed telephone numbers** for this same limited time period. The illegally spoofed calling numbers disguised calls as legitimate call traffic from local, state, and federal government agencies within the United States, and misrepresented callers’ affiliations with law enforcement agencies and private sector entities. Each call made using an illegally spoofed calling telephone number appears to have violated the TSR, 16 C.F.R. § 310.4(a)(8), and the Truth in Caller ID: 47 U.S.C. § 227(e)(1) and 47 C.F.R. § 64.1604(a).

Further, after an analysis of a subset of recorded voicemail messages that corresponded with the call detail records, more than **196,060 calls contained unlawful or fraudulent content**, with each call’s content appearing to have violated the TSR, 16 C.F.R. § 310.3(a)(2)(iii), and/or the TCPA, 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B), 47 C.F.R. § 64.1200(a)(2)–(3).

Finally, information available from ZipDX indicates that All Access also attested to calls for a number of the same high-volume robocalling campaigns for which it received and/or continues to receive traceback notices from the ITG. For instance, in just the last few months, ZipDX identified **56 suspicious calls** transmitted by All Access **from 56 unique calling numbers**,⁸ exhibiting characteristics indicative of calls that are violations of federal and state laws; 95% of these calls were also made to numbers that have been registered on the National Do Not Call Registry.⁹

After reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force has concluded that All Access is and/or has been involved in, at a minimum, transmitting call traffic indicative of, and associated with, recurrent high-volume illegal and/or suspicious robocalling campaigns and/or practices, which conduct could subject All Access to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and state laws.

⁸ The use of many unique calling numbers for this volume of called numbers indicates a suspicious pattern in your call traffic of “snowshoeing” or “snowshoe spoofing,” which is a practice often employed by illegal robocallers and telemarketers to circumvent the protections of the STIR/SHAKEN call authentication framework by using significant quantities of unique numbers for caller IDs on a short-term or rotating basis in order to evade behavioral analytics detection, or to bypass or hinder call blocking or call labeling analytics based on the origination numbers. Telephone numbers used for snowshoeing sometimes cannot themselves receive incoming calls, which has the effect of impeding an audit of the legitimacy of these calling numbers.

⁹ Most calls captured by RRAPTOR are calls made to phone numbers that have been registered on the National Do Not Call Registry.

Overview of Select Relevant Laws

As All Access well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,¹⁰ the Telephone Consumer Protection Act,¹¹ and/or the Truth in Caller ID Act,¹² as well as state consumer protection statutes.

Telemarketing Sales Rule (15 U.S.C. §§ 6101–6108; 16 C.F.R. Part 310)

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act which directed the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices.¹³ Pursuant to this directive, the FTC promulgated the Telemarketing Sales Rule (“TSR”). It is a violation of the TSR for voice service providers to provide substantial assistance to customers that the provider “knows or consciously avoids knowing” are engaged in practices that violate TSR provisions against deceptive and abusive telemarketing acts or practices.¹⁴ State Attorneys General have concurrent authority with the FTC to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR.¹⁵

Telephone Consumer Protection Act (47 U.S.C. § 227; 47 C.F.R. §§ 64.1200 and 64.1604)

Under the Telephone Consumer Protection Act (“TCPA”), the FCC promulgated rules restricting calls made with automated telephone dialing systems and calls delivering artificial or prerecorded voice messages.¹⁶ Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.¹⁷ State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.¹⁸ The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,¹⁹ including those made with the “prior express consent” of the called party or with “prior express *written* consent” of the called party for telemarketing calls.²⁰ Note, however, the FCC has found in at least one instance that single consents purportedly given

¹⁰ 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4.

¹¹ 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

¹² 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

¹³ 15 U.S.C. § 6102.

¹⁴ 16 C.F.R. § 310.3(b).

¹⁵ 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

¹⁶ 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3).

¹⁷ 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2).

¹⁸ 47 U.S.C. § 227(g)(1).

¹⁹ 47 U.S.C. § 227(b)(1)(A)–(B), (b)(2)(B); 47 C.F.R. § 64.1200(a)(1)–(3), (a)(9).

²⁰ 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.²¹

Truth in Caller ID Act (47 U.S.C. § 227(e))

Under the federal Truth in Caller ID Act, it is generally unlawful for a person to “knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.”²² State Attorneys General have the authority to bring enforcement actions for violations of the Truth in Caller ID Act and its prohibition against illegal caller identification spoofing.²³ Such violative conduct can lead to assessments of civil penalties of up to \$10,000 for each violation, or three times that amount for each day of continuing violations.²⁴ Note that any penalties for violations of the Truth in Caller ID Act are in addition to those assessed for any other penalties provided for by the TCPA.²⁵

General Note regarding State Laws

In addition to their authority to enforce the above federal statutes, State Attorneys General are empowered to enforce their respective state laws regulating various aspects of the initiation and transmission of illegal robocall and telemarketing call traffic across the U.S. telephone

²¹ For example, in November 2022, the FCC issued an order requiring all voice service providers to block calls from provider Urth Access, LLC. In response to allegations concerning the transmission of illegal robocalls, Urth Access claimed to have obtained express consent for each of the calls. However, that consent stemmed from websites where consumers purportedly agreed to receive robocalls from over 5,000 “marketing partners” listed on a separate site. The FCC found this type of practice insufficient to constitute express consent to the marketing partners to contact the consumers. *See FCC Orders Voice Service Providers to Block Student Loan Robocalls*, <https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls> (Order); *FCC Issues Robocall Cease-and-Desist Letter to Urth Access*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-urth-access> (Cease-and-Desist Letter). We note that this decision is consistent with the FTC’s interpretation of the express consent requirement of the TSR. *See* Federal Register, Vol. 73 No. 169, 2008 at 51182, <https://www.govinfo.gov/content/pkg/FR-2008-08-29/pdf/E8-20253.pdf> (consumer’s agreement with a seller to receive calls delivering prerecorded messages is nontransferable); *FTC, Complying with the Telemarketing Sales Rule, The Written Agreement Requirement*, <https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement>; *but see, Insurance Marketing Coalition, Ltd. v. Federal Communications Commission*, -- F.4th --, 2025 WL 289152 (11th Cir. 2025) (vacating and remanding FCC rule requiring those wishing to make a telemarketing or advertising robocall to obtain (1) consent from one called party to one seller at a time; and (2) consent that is logically and topically related to the interaction that prompted the consent).

²² 47 U.S.C. § 227(e)(1); 47 C.F.R. § 64.1604.

²³ 47 U.S.C. § 227(e)(6).

²⁴ 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

²⁵ *Id.*

network. Voice service providers transmitting calls into and throughout the states are obligated to familiarize themselves with, and abide by, all applicable state laws.

Requested Action in Response to this Notice

As noted above, the Task Force is providing this Notice in order to memorialize some of its investigative findings to date. The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, and has been, accepted and transmitted by and through All Access's network, in order to ensure that your current business—and any subsequently-formed businesses—follow all applicable federal and state laws and regulations, including those referenced above. If subsequent investigation shows that All Access and/or its principals continue to assist customers by initiating and/or transmitting call traffic not dissimilar from the traffic highlighted in this Notice, the Task Force may decide to pursue an enforcement action against All Access, any later-formed business entities, and the principal owners and operators in common to both. Future action may also consist of referring the matter to the FCC for consideration of potential enforcement actions.²⁶

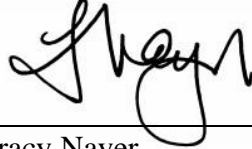
For your information, we have informed several of our federal law enforcement counterparts—including our colleagues at the FCC's Enforcement Bureau—of the Task Force's intention to issue this Notice to All Access. Finally, this Notice does not waive or otherwise preclude the Task Force from bringing an enforcement action related to conduct preceding the date

²⁶ The FCC's authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter, *see, e.g., FCC Orders Avid Telecom to Cease and Desist Robocalls* <https://www.fcc.gov/document/fcc-orders-avid-telecom-cess-and-desist-robocalls> (issued Jun. 7, 2023); *FCC Issues Robocall Cease-and-Desist Letter to PZ/Illum*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-pzillum> (issued Oct. 21, 2021), a K4 Public Notice, *see FCC Enforcement Bureau Notifies All U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting From One Eye LLC*, <https://www.fcc.gov/document/fcc-takes-repeat-robocall-offenders-attempts-evade-enforcement> (issued Feb. 15, 2023), a Notice of Apparent Liability, *see, e.g., John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948 (2020), *available at* https://docs.fcc.gov/public/attachments/FCC-20-74A1_Rcd.pdf, a Consumer Communications Information Services Threat ("C-CIST") Designation Notice, *see FCC [Enforcement Bureau] Issues C-CIST Classification for "Royal Tiger"*, <https://www.fcc.gov/document/fcc-eb-issues-c-cist-classification-royal-tiger> (issued May 13, 2024), or proceedings that may result in removal from the Robocall Mitigation Database, *see, e.g., Viettel Business Solutions Company, Etihad Etisalat (Mobily), Claude ICT Poland Sp. z o. o. dba TeleCube.PL, Nervill LTD, Textodog Inc. dba Textodog and Textodog Software Inc., Phone GS, Computer Integrated Solutions dba CIS IT & Engineering, Datacom Specialists, DomainerSuite, Inc., Evernex SMC PVT LTD, Humbolt Voip, and My Taxi Ride Inc.*, Removal Order, 39 FCC Rcd 1319 (2024), *available at* <https://www.fcc.gov/document/fcc-removes-12-entities-robocall-mitigation-database>, the latter of which—if completed—would require all intermediate providers and terminating voice service providers to cease accepting your call traffic.

of this Notice, including conduct that resulted in violations related to the call traffic referenced in this Notice.

The Task Force remains steadfast in its resolve to meaningfully curb illegal robocall traffic. Please direct any inquiries regarding this Notice to my attention at tnayer@ncdoj.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "Tracy Nayer", written over a horizontal line.

Tracy Nayer
Special Deputy Attorney General
Consumer Protection Division
North Carolina Department of Justice

JEFF JACKSON
ATTORNEY GENERAL



TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL
TNAYER@NCDOJ.GOV

April 9, 2025

Bryan Hertz
Robert Hertz
Telcentris, Inc. dba Voxox
c/o Michael P. Donahue
Marashlian & Donahue, PLLC
The CommLaw Group
1430 Spring Hill Road, Suite 310
Tysons, Virginia 22102

Sent via certified mail, return receipt requested, and via email to mpd@CommLawGroup.com

Re: SECOND AND FINAL NOTICE LETTER from the Anti-Robocall Multistate Litigation Task Force Concerning Telcentris, Inc. dba Voxox's Continued Involvement in Suspected Illegal Robocall Traffic

Dear Messrs. Hertz:

The Anti-Robocall Multistate Litigation Task Force's ("Task Force")¹ investigation of Telcentris, Inc. dba Voxox ("Voxox")² has shown that Voxox has transmitted, and continues to transmit, suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is the Task Force's second and final attempt to informally apprise you of the Task Force's concerns regarding Voxox call traffic, and to caution Voxox that it should scrutinize the call traffic of its current customers, evaluate the efficacy of its existing robocall mitigation policies, and cease transmitting illegal traffic on behalf of its current customers.

¹ The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall ecosystem that are identified as being responsible for significant volumes of illegal and fraudulent robocall traffic routed into and across the country.

² Telcentris, Inc. dba Voxox—FCC Registration No. 0016106460; Robocall Mitigation Database No. RMD0001881—"Voxox") is a Delaware corporation, registered in California as a foreign corporation. Bryan Hertz is identified as Voxox's Chief Executive Officer in the FCC's Form 499 Filer Database. FCC Form 499 Filer Database, <https://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=826490> (last visited Mar. 19, 2025). Robert Hertz is identified as Voxox's Chief Executive Officer in the FCC's Robocall Mitigation Database.

The Task Force provides this Notice in order to memorialize some of its investigative findings to date.

Task Force’s Findings Regarding Voxox’s Call Traffic

As you are aware, on August 1, 2022, the Task Force issued its Civil Investigative Demand (“CID”) to Voxox to identify, investigate, and mitigate suspected illegal call traffic that is or was accepted onto, and transmitted across, Voxox’s network.

On March 17, 2023, Voxox was issued a Cease-and-Desist Demand³ from the Federal Trade Commission (“FTC”). The FTC’s Cease-and-Desist provided that Voxox was knowingly routing and transmitting illegal robocall traffic identified therein.⁴ The FTC’s Cease-and-Desist referenced applicable federal laws and rules, and Voxox’s legal obligations under the same.

On November 3, 2023, the Task Force issued a Notice to Voxox (“2023 Task Force Notice”) memorializing some of the Task Force’s findings concerning Voxox’s call traffic, informing you of the Task Force’s continuing concerns regarding your call traffic, and cautioning Voxox that it should cease transmitting any illegal traffic immediately. Based on pertinent analyses and information available to the Task Force, it appears that Voxox has continued to transmit calls associated with high-volume illegal and/or suspicious robocall campaigns.

As noted in the 2023 Task Force Notice, as part of its investigation into the transmission of illegal robocalls and the providers and entities that originate and/or route them, the Task Force regularly reviews call traffic information from several industry sources, including USTelecom’s Industry Traceback Group (“ITG”)⁵ and ZipDX LLC (“ZipDX”)⁶.

³ FTC, *Cease and Desist Demand to Telcentris, Inc., also d/b/a Voxox*, https://www.ftc.gov/system/files/ftc_gov/pdf/pointofnoentry-telcentrisceasedesistletterfinaljms.pdf (hereinafter “FTC’s Cease-and-Desist”).

⁴ FTC’s Cease-and-Desist at 1–2.

⁵ Established in 2015, the ITG is a private collaborative industry group—composed of providers across wireline, wireless, VOIP, and cable services—that traces and identifies the sources of suspected illegal and suspicious robocalls. In December 2019, Congress enacted the Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) to combat the scourge of unlawful robocalls. *See* Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019). Following its enactment, the Federal Communications Commission designated the ITG as the official private-led traceback consortium charged with leading the voice communications industry’s efforts to trace the origin of suspected illegal robocalls through various communications networks through tracebacks. *See* 47 C.F.R. § 64.1203.

⁶ ZipDX is a provider of web- and phone-based collaboration services, which also focuses resources on developing and making technology available that is directed at mitigating illegal robocalls and other telephone-based fraud and abuse. ZipDX’s proprietary tool “RRAPTOR” is one such technology, which is an automated robocall surveillance tool that captures call recordings

Call traffic data from the ITG shows that it issued at least **440 traceback notices** to Voxox since January 2019 for calls it accepted and/or transmitted onto and across the U.S. telephone network. These notices from the ITG cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning SSA government imposter, utilities disconnect, financial/business impersonations, Amazon, student loans, and others, with Voxox identified as serving in various roles in the call path. At least **173 traceback notices** were issued since August 2022—after the Task Force issued its CID to Voxox—and, of those, still more than **50 traceback notices** were issued since the 2023 Task Force Notice. While the traceback notices issued since August 2022 show that Voxox is no longer regularly identified as the point-of-entry or gateway⁷ provider for this traffic, there is still a smaller portion of this traffic for which Voxox is identified as the immediate downstream provider to the originating provider or the originating provider itself. Because the ITG estimates that each traced call is representative of a large volume of similar illegal and/or suspicious calls,⁸ Voxox is likely continuing to cause significant volumes of illegal and/or suspicious robocalls to ultimately reach U.S. consumers, despite traceback notifications from the ITG of this identified and suspected illegal call traffic.

Information available from ZipDX indicates that Voxox also attested to calls for a number of the same high-volume robocalling campaigns for which it received and/or continues to receive traceback notices from the ITG. For instance, during the last ten months, ZipDX identified **189 suspicious calls** transmitted by Voxox **from 189 unique calling numbers**,⁹ exhibiting

and information for calls largely associated with high-volume suspicious calling campaigns, and identifies the providers who have affixed their SHAKEN signatures to each of the captured calls, indicating that the provider is in the call path and whether those providers have attested to knowing the calling party who made the suspicious call and/or knowing of the calling party's right to use that calling number to make that suspicious call. See ZipDX, What is RRAPTOR?, <https://legalcallsonly.org/what-is-rraptor/> (last visited Oct. 17, 2024).

⁷ *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, 87 FR 42916, 42917–18, para. 7 (2022) (defining a “gateway provider” as “a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider”).

⁸ USTelecom, *Industry Traceback Group Policies and Procedures*, at 4 (last revised April 2022) (*ITG Policies & Procedures*) (defining “campaign” as “[a] group of calls with identical or nearly identical messaging as determined by the content and calling patterns of the caller,” where “[a] single Campaign often represents hundreds of thousands or millions of calls”), available at <https://r01986.a2cdn1.secureserver.net/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf>.

⁹ The use of many unique calling numbers for this volume of called numbers indicates a suspicious pattern in your call traffic of “snowshoeing” or “snowshoe spoofing,” which is a practice often employed by illegal robocallers and telemarketers to circumvent the protections of the STIR/SHAKEN call authentication framework by using significant quantities of unique numbers for caller IDs on a short-term or rotating basis in order to evade behavioral analytics detection, or

characteristics indicative of calls that are violations of federal and state laws; 95% of these calls were also made to numbers that have been registered on the National Do Not Call Registry.¹⁰

Lastly, analysis of a portion of Voxox's likely involvement in the routing of nationwide call traffic concerning Amazon/Apple imposter robocalls was assessed. Between September 2020 and October 2022, among a nationwide sample of over 2.59 million transcribed and recorded Amazon/Apple imposter robocalls, **more than 94,500 of these Amazon/Apple imposter robocalls are estimated to be attributable to Voxox.** Thus, of the more than 1.2 billion estimated Amazon/Apple imposter robocalls reaching consumers across the country in this sample during this period, **approximately 47.7 million of these scam robocalls are estimated to be attributable to Voxox.**

A similar analysis of Voxox's likely involvement in the routing of nationwide call traffic concerning SSA/IRS government imposter robocalls was assessed. Between July 2019 and July 2022, among a nationwide sample of over 5.3 million transcribed and recorded SSA/IRS government imposter robocalls, **more than 232,000 of these SSA/IRS government imposter robocalls are estimated to be attributable to Voxox.** Thus, of the over 2.65 billion estimated SSA/IRS government imposter robocalls reaching consumers across the country in this sample during this period, **approximately 116 million of these scam robocalls are estimated to be attributable to Voxox.**

After reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force has concluded that Voxox is and/or has been involved in, at a minimum, transmitting call traffic indicative of, and associated with, recurrent high-volume illegal and/or suspicious robocalling campaigns and/or practices, which conduct could subject Voxox to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and state laws.

Overview of Select Relevant Laws

As Voxox well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,¹¹ the Telephone Consumer Protection Act,¹² and/or the Truth in Caller ID Act,¹³ as well as state consumer protection statutes.

to bypass or hinder call blocking or call labeling analytics based on the origination numbers. Telephone numbers used for snowshoeing sometimes cannot themselves receive incoming calls, which has the effect of impeding an audit of the legitimacy of these calling numbers.

¹⁰ Most calls captured by RRAPTOR are calls made to phone numbers that have been registered on the National Do Not Call Registry.

¹¹ 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4.

¹² 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

¹³ 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

Telemarketing Sales Rule (15 U.S.C. §§ 6101–6108; 16 C.F.R. Part 310)

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act which directed the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices.¹⁴ Pursuant to this directive, the FTC promulgated the Telemarketing Sales Rule (“TSR”). It is a violation of the TSR for voice service providers to provide substantial assistance to customers that the provider “knows or consciously avoids knowing” are engaged in practices that violate TSR provisions against deceptive and abusive telemarketing acts or practices.¹⁵ State Attorneys General have concurrent authority with the FTC to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR.¹⁶

Telephone Consumer Protection Act (47 U.S.C. § 227; 47 C.F.R. §§ 64.1200 and 64.1604)

Under the Telephone Consumer Protection Act (“TCPA”), the FCC promulgated rules restricting calls made with automated telephone dialing systems and calls delivering artificial or prerecorded voice messages.¹⁷ Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.¹⁸ State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.¹⁹ The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,²⁰ including those made with the “prior express consent” of the called party or with “prior express *written* consent” of the called party for telemarketing calls.²¹ Note, however, the FCC has found in at least one instance that single consents purportedly given by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.²²

¹⁴ 15 U.S.C. § 6102.

¹⁵ 16 C.F.R. § 310.3(b).

¹⁶ 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

¹⁷ 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3).

¹⁸ 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2).

¹⁹ 47 U.S.C. § 227(g)(1).

²⁰ 47 U.S.C. § 227(b)(1)(A)–(B), (b)(2)(B); 47 C.F.R. § 64.1200(a)(1)–(3), (a)(9).

²¹ 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

²² For example, in November 2022, the FCC issued an order requiring all voice service providers to block calls from provider Urth Access, LLC. In response to allegations concerning the transmission of illegal robocalls, Urth Access claimed to have obtained express consent for each of the calls. However, that consent stemmed from websites where consumers purportedly agreed to receive robocalls from over 5,000 “marketing partners” listed on a separate site. The FCC found this type of practice insufficient to constitute express consent to the marketing partners to contact the consumers. See *FCC Orders Voice Service Providers to Block Student Loan Robocalls*, <https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls> (Order); *FCC Issues Robocall Cease-and-Desist Letter to Urth Access*,

Truth in Caller ID Act (47 U.S.C. § 227(e))

Under the federal Truth in Caller ID Act, it is generally unlawful for a person to “knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.”²³ State Attorneys General have the authority to bring enforcement actions for violations of the Truth in Caller ID Act and its prohibition against illegal caller identification spoofing.²⁴ Such violative conduct can lead to assessments of civil penalties of up to \$10,000 for each violation, or three times that amount for each day of continuing violations.²⁵ Note that any penalties for violations of the Truth in Caller ID Act are in addition to those assessed for any other penalties provided for by the TCPA.²⁶

General Note regarding State Laws

In addition to their authority to enforce the above federal statutes, State Attorneys General are empowered to enforce their respective state laws regulating various aspects of the initiation and transmission of illegal robocall and telemarketing call traffic across the U.S. telephone network. Voice service providers transmitting calls into and throughout the states are obligated to familiarize themselves with, and abide by, all applicable state laws.

Requested Action in Response to this Notice

As noted above, the Task Force is providing this Notice in order to memorialize some of its investigative findings to date. The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, and has been, accepted and transmitted by and through Voxox’s network, in order to ensure that your current business—and any subsequently-formed businesses—follow all applicable federal and state laws and regulations, including those referenced above. If subsequent investigation shows that Voxox and/or its principals continue to assist customers by initiating and/or transmitting call

<https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-urth-access> (Cease-and-Desist Letter). We note that this decision is consistent with the FTC’s interpretation of the express consent requirement of the TSR. *See* Federal Register, Vol. 73 No. 169, 2008 at 51182, <https://www.govinfo.gov/content/pkg/FR-2008-08-29/pdf/E8-20253.pdf> (consumer’s agreement with a seller to receive calls delivering prerecorded messages is nontransferable); *FTC, Complying with the Telemarketing Sales Rule, The Written Agreement Requirement*, <https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement>; *but see, Insurance Marketing Coalition, Ltd. v. Federal Communications Commission*, -- F.4th --, 2025 WL 289152 (11th Cir. 2025) (vacating and remanding FCC rule requiring those wishing to make a telemarketing or advertising robocall to obtain (1) consent from one called party to one seller at a time; and (2) consent that is logically and topically related to the interaction that prompted the consent).

²³ 47 U.S.C. § 227(e)(1); 47 C.F.R. § 64.1604.

²⁴ 47 U.S.C. § 227(e)(6).

²⁵ 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

²⁶ *Id.*

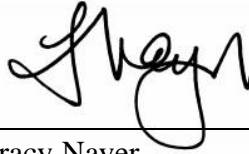
traffic not dissimilar from the traffic highlighted in this Notice, the Task Force may decide to pursue an enforcement action against Voxox, any later-formed business entities, and the principal owners and operators in common to both. Future action may also consist of referring the matter to the FCC for consideration of potential enforcement actions.²⁷

For your information, we have informed several of our federal law enforcement counterparts—including our colleagues at the FCC’s Enforcement Bureau—of the Task Force’s intention to issue this Notice to Voxox. Finally, this Notice does not waive or otherwise preclude the Task Force from bringing an enforcement action related to conduct preceding the date of this Notice, including conduct that resulted in violations related to the call traffic referenced in this Notice.

²⁷ The FCC’s authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter, *see, e.g., FCC Orders Avid Telecom to Cease and Desist Robocalls* <https://www.fcc.gov/document/fcc-orders-avid-telecom-cess-and-desist-robocalls> (issued Jun. 7, 2023); *FCC Issues Robocall Cease-and-Desist Letter to PZ/Illum*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-pzillum> (issued Oct. 21, 2021), a K4 Public Notice, *see FCC Enforcement Bureau Notifies All U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting From One Eye LLC*, <https://www.fcc.gov/document/fcc-takes-repeat-robocall-offenders-attempts-evade-enforcement> (issued Feb. 15, 2023), a Notice of Apparent Liability, *see, e.g., John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948 (2020), *available at* https://docs.fcc.gov/public/attachments/FCC-20-74A1_Rcd.pdf, a Consumer Communications Information Services Threat (“C-CIST”) Designation Notice, *see FCC [Enforcement Bureau] Issues C-CIST Classification for “Royal Tiger”*, <https://www.fcc.gov/document/fcc-eb-issues-c-cist-classification-royal-tiger> (issued May 13, 2024), or proceedings that may result in removal from the Robocall Mitigation Database, *see, e.g., Viettel Business Solutions Company, Etihad Etisalat (Mobily), Claude ICT Poland Sp. z o. o. dba TeleCube.PL, Nervill LTD, Textodog Inc. dba Textodog and Textodog Software Inc., Phone GS, Computer Integrated Solutions dba CIS IT & Engineering, Datacom Specialists, DomainerSuite, Inc., Evernex SMC PVT LTD, Humbolt Voip, and My Taxi Ride Inc.*, Removal Order, 39 FCC Rcd 1319 (2024), *available at* <https://www.fcc.gov/document/fcc-removes-12-entities-robocall-mitigation-database>, the latter of which—if completed—would require all intermediate providers and terminating voice service providers to cease accepting your call traffic.

The Task Force remains steadfast in its resolve to meaningfully curb illegal robocall traffic. Please direct any inquiries regarding this Notice to my attention at tnayer@ncdoj.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "Tracy Nayer", written over a horizontal line.

Tracy Nayer
Special Deputy Attorney General
Consumer Protection Division
North Carolina Department of Justice

JEFF JACKSON
ATTORNEY GENERAL



TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL
TNAYER@NCDOJ.GOV

April 9, 2025

Eric Engbers, CEO
NGL Communications LLC
c/o Philip Macres
Klein Law Group PLLC
1250 Connecticut Ave. N.W., Suite 700
Washington, D.C. 20036

Sent via certified mail, return receipt requested, and via email to PMacres@KleinLawPLLC.com

Re: SECOND AND FINAL NOTICE LETTER from the Anti-Robocall Multistate Litigation Task Force Concerning NGL Communications LLC's Continued Involvement in Suspected Illegal Robocall Traffic

Dear Mr. Engbers:

The Anti-Robocall Multistate Litigation Task Force's ("Task Force")¹ investigation of NGL Communications LLC ("NGL")² has shown that NGL has transmitted, and continues to transmit, suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is the Task Force's second and final attempt to informally apprise you of the Task Force's concerns regarding NGL's call traffic, and to caution NGL that it should scrutinize the call traffic of its current customers, evaluate the efficacy of its existing robocall mitigation policies, and cease transmitting illegal traffic on behalf of its current customers.

The Task Force provides this Notice in order to memorialize some of its investigative findings to date.

¹ The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall ecosystem that are identified as being responsible for significant volumes of illegal and fraudulent robocall traffic routed into and across the country.

² NGL Communications, LLC—FCC Registration No. 27599695; Robocall Mitigation Database No. RMD0001774—"NGL") is a North Carolina limited liability company. Eric Engbers serves as NGL's Chief Executive Officer. Derek Dempsay is VP of Operations and Jeremy Kelley is VP of Business Development. The FCC's Robocall Mitigation Database identifies Oregon-based IP Link Technologies Group, Inc. as NGL's principal, affiliate, subsidiary, or parent company.

Task Force’s Findings Regarding NGL’s Call Traffic

As you are aware, on August 1, 2022, the Task Force issued its Civil Investigative Demand (“CID”) to NGL to identify, investigate, and mitigate suspected illegal call traffic that is or was accepted onto, and transmitted across, NGL’s network. On November 3, 2023, the Task Force issued a Notice to NGL (“2023 Task Force Notice”) memorializing some of the Task Force’s findings concerning NGL’s call traffic, informing you of the Task Force’s continuing concerns regarding your call traffic, and cautioning NGL that it should cease transmitting any illegal traffic immediately. Based on pertinent analyses and information available to the Task Force, it appears that NGL has continued to transmit calls associated with high-volume illegal and/or suspicious robocall campaigns.

During the course of its investigation of NGL, the Task Force requested the production of call detail records for all call traffic sent to and/or through your network or which you originated on behalf of your customers during a certain time period. Additionally, as noted in the 2023 Task Force Notice, as part of its investigation into the transmission of illegal robocalls and the providers and entities that originate and/or route them, the Task Force regularly reviews call traffic information from several industry sources, including USTelecom’s Industry Traceback Group (“ITG”).³

Call traffic data from the ITG shows that it issued at least **365 traceback notices** to NGL since January 2019 for calls it accepted and/or transmitted onto and across the U.S. telephone network. These notices from the ITG cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning government imposters and impersonations, COVID financial relief, Amazon, student loan forgiveness, debt relief, DirecTV discounts, credit card interest rate reductions, and others, with NGL identified as serving in various roles in the call path. At least **192 traceback notices** were issued since August 2022—after the Task Force issued its CID to NGL—and, of those, still about **50% of those traceback notices** were issued since the 2023 Task Force Notice. While the traceback notices issued since August 2022 show that NGL is not being identified as the point-of-entry or gateway⁴ provider for this traffic, there is still a portion of this

³ Established in 2015, the ITG is a private collaborative industry group—composed of providers across wireline, wireless, VOIP, and cable services—that traces and identifies the sources of suspected illegal and suspicious robocalls. In December 2019, Congress enacted the Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) to combat the scourge of unlawful robocalls. *See* Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019). Following its enactment, the Federal Communications Commission designated the ITG as the official private-led traceback consortium charged with leading the voice communications industry’s efforts to trace the origin of suspected illegal robocalls through various communications networks through tracebacks. *See* 47 C.F.R. § 64.1203.

⁴ *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, 87 FR 42916, 42917–18, para. 7 (2022) (defining a “gateway provider” as “a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider”).

traffic for which NGL is identified as the immediate downstream provider to the originating provider. Because the ITG estimates that each traced call is representative of a large volume of similar illegal and/or suspicious calls,⁵ NGL is likely continuing to cause significant volumes of illegal and/or suspicious robocalls to ultimately reach U.S. consumers, despite traceback notifications from the ITG of this identified and suspected illegal call traffic.

Further, an analysis of a set of call detail records⁶ from NGL's nationwide call traffic between the end of December 2020 and July 2022 shows that more than **1.135 billion calls were made using invalid Caller ID numbers**, which means the calling numbers making the calls used a combination of numbers that were not assigned and/or recognized as valid by the North American Numbering Plan Administrator. Each call made using an invalid calling telephone number appears to have violated the Truth in Caller ID, 47 U.S.C. 227(e)(1) and 47 C.F.R. 64.1604(a), and the TCPA, 47 C.F.R. § 64.1200(n)(4)–(5).

Additionally, NGL's nationwide call traffic included more than **7.73 million calls using illegally spoofed telephone numbers** for this same limited time period. The illegally spoofed calling numbers disguised calls as legitimate call traffic from local, state, and federal government agencies within the United States, and misrepresented callers' affiliations with law enforcement agencies and private sector entities. Each call made using an illegally spoofed calling telephone number appears to have violated the TSR, 16 C.F.R. § 310.4(a)(8), and the Truth in Caller ID: 47 U.S.C. § 227(e)(1) and 47 C.F.R. § 64.1604(a).

Finally, after an analysis of a subset of recorded voicemail messages that corresponded with the call detail records, more than **533,900 calls contained unlawful or fraudulent content**,

⁵ USTelecom, *Industry Traceback Group Policies and Procedures*, at 4 (last revised April 2022) (*ITG Policies & Procedures*) (defining "campaign" as "[a] group of calls with identical or nearly identical messaging as determined by the content and calling patterns of the caller," where "[a] single Campaign often represents hundreds of thousands or millions of calls"), *available at* <https://r01986.a2cdn1.secureserver.net/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf>.

⁶ Call detail records or "CDRs" are automatically generated records of each attempted or completed call that reaches and/or crosses a voice service provider's network. CDRs generally include the following information:

- a. The date and time of the call attempt;
- b. The duration of the call (calls that fail to connect are generally denoted by a zero-second duration);
- c. The intended call recipient's telephone number;
- d. The originating or calling number from which the call was placed (which may be a real number or may be spoofed);
- e. An identifier such as a name or account number for the upstream provider that sent the call attempt to the provider's network; and
- f. An identifier for the downstream provider to which the provider attempts to route the call.

with each call's content appearing to have violated the TSR, 16 C.F.R. § 310.3(a)(2)(iii), and/or the TCPA, 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B), 47 C.F.R. § 64.1200(a)(2)–(3).

Lastly, analysis of a portion of NGL's likely involvement in the routing of nationwide call traffic concerning Amazon/Apple imposter robocalls was assessed. Between January 2022 and July 2024, among a nationwide sample of over 1.47 million transcribed and recorded Amazon/Apple imposter robocalls, **approximately 17,700 of these Amazon/Apple imposter robocalls are estimated to be attributable to NGL.** Thus, of the more than 736.5 million estimated Amazon/Apple imposter robocalls reaching consumers across the country in this sample during this period, **approximately 8.88 million of these scam robocalls are estimated to be attributable to NGL.**

A similar analysis of NGL's likely involvement in the routing of nationwide call traffic concerning SSA/IRS government imposter robocalls was assessed. Between September 2020 and March 2022, among a nationwide sample of over 3.9 million transcribed and recorded SSA/IRS government imposter robocalls, **more than 85,100 of these SSA/IRS government imposter robocalls are estimated to be attributable to NGL.** Thus, of the over 1.96 billion estimated SSA/IRS government imposter robocalls reaching consumers across the country in this sample during this period, **approximately 42.5 million of these scam robocalls are estimated to be attributable to NGL.**

After reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force has concluded that NGL is and/or has been involved in, at a minimum, transmitting call traffic indicative of, and associated with, recurrent high-volume illegal and/or suspicious robocalling campaigns and/or practices, which conduct could subject NGL to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and state laws.

Overview of Select Relevant Laws

As NGL well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,⁷ the Telephone Consumer Protection Act,⁸ and/or the Truth in Caller ID Act,⁹ as well as state consumer protection statutes.

Telemarketing Sales Rule (15 U.S.C. §§ 6101–6108; 16 C.F.R. Part 310)

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act which directed the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices.¹⁰ Pursuant to this directive, the FTC promulgated the Telemarketing Sales Rule (“TSR”). It is a violation of the TSR for voice service providers to provide substantial assistance

⁷ 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4.

⁸ 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

⁹ 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

¹⁰ 15 U.S.C. § 6102.

to customers that the provider “knows or consciously avoids knowing” are engaged in practices that violate TSR provisions against deceptive and abusive telemarketing acts or practices.¹¹ State Attorneys General have concurrent authority with the FTC to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR.¹²

Telephone Consumer Protection Act (47 U.S.C. § 227; 47 C.F.R. §§ 64.1200 and 64.1604)

Under the Telephone Consumer Protection Act (“TCPA”), the FCC promulgated rules restricting calls made with automated telephone dialing systems and calls delivering artificial or prerecorded voice messages.¹³ Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.¹⁴ State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.¹⁵ The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,¹⁶ including those made with the “prior express consent” of the called party or with “prior express *written* consent” of the called party for telemarketing calls.¹⁷ Note, however, the FCC has found in at least one instance that single consents purportedly given by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.¹⁸

¹¹ 16 C.F.R. § 310.3(b).

¹² 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

¹³ 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3).

¹⁴ 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2).

¹⁵ 47 U.S.C. § 227(g)(1).

¹⁶ 47 U.S.C. § 227(b)(1)(A)–(B), (b)(2)(B); 47 C.F.R. § 64.1200(a)(1)–(3), (a)(9).

¹⁷ 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

¹⁸ For example, in November 2022, the FCC issued an order requiring all voice service providers to block calls from provider Urth Access, LLC. In response to allegations concerning the transmission of illegal robocalls, Urth Access claimed to have obtained express consent for each of the calls. However, that consent stemmed from websites where consumers purportedly agreed to receive robocalls from over 5,000 “marketing partners” listed on a separate site. The FCC found this type of practice insufficient to constitute express consent to the marketing partners to contact the consumers. See *FCC Orders Voice Service Providers to Block Student Loan Robocalls*, <https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls> (Order); *FCC Issues Robocall Cease-and-Desist Letter to Urth Access*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-urth-access> (Cease-and-Desist Letter). We note that this decision is consistent with the FTC’s interpretation of the express consent requirement of the TSR. See Federal Register, Vol. 73 No. 169, 2008 at 51182, <https://www.govinfo.gov/content/pkg/FR-2008-08-29/pdf/E8-20253.pdf> (consumer’s agreement with a seller to receive calls delivering prerecorded messages is nontransferable); *FTC, Complying with the Telemarketing Sales Rule, The Written Agreement Requirement*, <https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales->

Truth in Caller ID Act (47 U.S.C. § 227(e))

Under the federal Truth in Caller ID Act, it is generally unlawful for a person to “knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.”¹⁹ State Attorneys General have the authority to bring enforcement actions for violations of the Truth in Caller ID Act and its prohibition against illegal caller identification spoofing.²⁰ Such violative conduct can lead to assessments of civil penalties of up to \$10,000 for each violation, or three times that amount for each day of continuing violations.²¹ Note that any penalties for violations of the Truth in Caller ID Act are in addition to those assessed for any other penalties provided for by the TCPA.²²

General Note regarding State Laws

In addition to their authority to enforce the above federal statutes, State Attorneys General are empowered to enforce their respective state laws regulating various aspects of the initiation and transmission of illegal robocall and telemarketing call traffic across the U.S. telephone network. Voice service providers transmitting calls into and throughout the states are obligated to familiarize themselves with, and abide by, all applicable state laws.

Requested Action in Response to this Notice

As noted above, the Task Force is providing this Notice in order to memorialize some of its investigative findings to date. The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, and has been, accepted and transmitted by and through NGL’s network, in order to ensure that your current business—and any subsequently-formed businesses—follow all applicable federal and state laws and regulations, including those referenced above. If subsequent investigation shows that NGL and/or its principals continue to assist customers by initiating and/or transmitting call traffic not dissimilar from the traffic highlighted in this Notice, the Task Force may decide to pursue an enforcement action against NGL, any later-formed business entities, and the principal owners and

[rule#writtenagreement](#); but see, *Insurance Marketing Coalition, Ltd. v. Federal Communications Commission*, -- F.4th --, 2025 WL 289152 (11th Cir. 2025) (vacating and remanding FCC rule requiring those wishing to make a telemarketing or advertising robocall to obtain (1) consent from one called party to one seller at a time; and (2) consent that is logically and topically related to the interaction that prompted the consent).

¹⁹ 47 U.S.C. § 227(e)(1); 47 C.F.R. § 64.1604.

²⁰ 47 U.S.C. § 227(e)(6).

²¹ 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

²² *Id.*

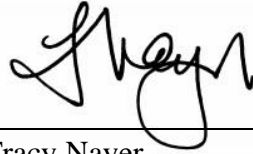
operators in common to both. Future action may also consist of referring the matter to the FCC for consideration of potential enforcement actions.²³

For your information, we have informed several of our federal law enforcement counterparts—including our colleagues at the FCC’s Enforcement Bureau—of the Task Force’s intention to issue this Notice to NGL. Finally, this Notice does not waive or otherwise preclude the Task Force from bringing an enforcement action related to conduct preceding the date of this Notice, including conduct that resulted in violations related to the call traffic referenced in this Notice.

²³ The FCC’s authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter, *see, e.g., FCC Orders Avid Telecom to Cease and Desist Robocalls* <https://www.fcc.gov/document/fcc-orders-avid-telecom-cess-and-desist-robocalls> (issued Jun. 7, 2023); *FCC Issues Robocall Cease-and-Desist Letter to PZ/Illum*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-pzillum> (issued Oct. 21, 2021), a K4 Public Notice, *see FCC Enforcement Bureau Notifies All U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting From One Eye LLC*, <https://www.fcc.gov/document/fcc-takes-repeat-robocall-offenders-attempts-evade-enforcement> (issued Feb. 15, 2023), a Notice of Apparent Liability, *see, e.g., John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948 (2020), *available at* https://docs.fcc.gov/public/attachments/FCC-20-74A1_Rcd.pdf, a Consumer Communications Information Services Threat (“C-CIST”) Designation Notice, *see FCC [Enforcement Bureau] Issues C-CIST Classification for “Royal Tiger”*, <https://www.fcc.gov/document/fcc-eb-issues-c-cist-classification-royal-tiger> (issued May 13, 2024), or proceedings that may result in removal from the Robocall Mitigation Database, *see, e.g., Viettel Business Solutions Company, Etihad Etisalat (Mobily), Claude ICT Poland Sp. z o. o. dba TeleCube.PL, Nervill LTD, Textodog Inc. dba Textodog and Textodog Software Inc., Phone GS, Computer Integrated Solutions dba CIS IT & Engineering, Datacom Specialists, DomainerSuite, Inc., Evernex SMC PVT LTD, Humbolt Voip, and My Taxi Ride Inc.*, Removal Order, 39 FCC Rcd 1319 (2024), *available at* <https://www.fcc.gov/document/fcc-removes-12-entities-robocall-mitigation-database>, the latter of which—if completed—would require all intermediate providers and terminating voice service providers to cease accepting your call traffic.

The Task Force remains steadfast in its resolve to meaningfully curb illegal robocall traffic. Please direct any inquiries regarding this Notice to my attention at tnayer@ncdoj.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "Tracy Nayer", written over a horizontal line.

Tracy Nayer
Special Deputy Attorney General
Consumer Protection Division
North Carolina Department of Justice

JEFF JACKSON
ATTORNEY GENERAL



TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL
TNAYER@NCDOJ.GOV

April 9, 2025

Vitaly Potapov
Yechiel Ross
RSCom Ltd.
RSCom Business, LLC
c/o Corporation Service Company
1090 Vermont Avenue, NW
Washington DC 20005

Sent via certified mail, return receipt requested, and via email to vitaly@rscombusiness.com, robert.musgrove@rsc.com.us, info@rsc.com.ca

Re: SECOND AND FINAL NOTICE LETTER from the Anti-Robocall Multistate Litigation Task Force Concerning RSCom Ltd. and RSCom Business, LLC's Continued Involvement in Suspected Illegal Robocall Traffic

Dear Messrs. Potapov and Ross:

The Anti-Robocall Multistate Litigation Task Force's ("Task Force")¹ investigation of RSCom Ltd. and RSCom Business, LLC ("RSCom")² has shown that RSCom has transmitted, and

¹ The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall ecosystem that are identified as being responsible for significant volumes of illegal and fraudulent robocall traffic routed into and across the country.

² RSCom Ltd—FCC Registration No. 0030982169; Robocall Mitigation Database No. RMD0002444—is a foreign corporation that provides the same Canadian business address in both the FCC Robocall Mitigation Database ("RMD") and Form 499 Filer Database ("499 Database").
FCC Form 499 Filer Database,
<https://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=831882> (last visited Mar. 19, 2025).
The RMD identifies Yechiel Ross as RSCom Ltd's Chief Executive Officer, while the 499 Database identifies Vitaly Potapov as its CEO. RSCom Business, LLC—FCC Registration No. 0031023468; Robocall Mitigation Database No. RMD0002449—provides a Canadian address in the 499 Database and identifies RSCom Holdings LLC as its holding company, but attests in the RMD that it is not a foreign voice service provider and provides a business address in Dover, Delaware.
FCC Form 499 Filer Database,
<https://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=833889> (last visited Mar. 19, 2025).
The RMD and 499 Database identify Vitaly Potapov as RSCom Business, LLC's Managing Director and CEO, respectively. While neither entity's RMD includes a filed Robocall Mitigation

continues to transmit, suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is the Task Force’s second and final attempt to informally apprise you of the Task Force’s concerns regarding RSCoM call traffic, and to caution RSCoM that it should scrutinize the call traffic of its current customers, evaluate the efficacy of its existing robocall mitigation policies, and cease transmitting illegal traffic on behalf of its current customers.

The Task Force provides this Notice in order to memorialize some of its investigative findings to date.

Task Force’s Findings Regarding RSCoM’s Call Traffic

As you are aware, on March 17, 2021, RSCoM was issued a Cease-and-Desist Notice³ from the Federal Communications Commission (“FCC”) and, on May 10, 2022, RSCoM was issued a Warning Regarding Assisting and Facilitating Illegal Robocalls⁴ from the Federal Trade Commission (“FTC”). The FCC’s Cease-and-Desist provided that RSCoM was “apparently transmitting illegal robocall traffic on behalf of one or more of its clients” for “multiple illegal robocall campaigns.”⁵ The FTC’s Warning Letter provided that RSCoM was knowingly routing and transmitting illegal robocall traffic identified therein between January 19, 2021, and March 3, 2022.⁶ Both the FCC’s Cease-and-Desist and the FTC’s Warning Letter referenced applicable federal laws and rules, and RSCoM’s legal obligations under the same.

On August 1, 2022, the Task Force issued its Civil Investigative Demand (“CID”) to RSCoM to identify, investigate, and mitigate suspected illegal call traffic that is or was accepted onto, and transmitted across, RSCoM’s network. On November 3, 2023, the Task Force issued a Notice to RSCoM (“2023 Task Force Notice”) memorializing some of the Task Force’s findings concerning RSCoM’s call traffic, informing you of the Task Force’s continuing concerns regarding your call traffic, and cautioning RSCoM that it should cease transmitting any illegal traffic immediately. Based on pertinent analyses and information available to the Task Force, it appears that RSCoM has continued to transmit calls associated with high-volume illegal and/or suspicious robocall campaigns.

Plan, both RMD entries provide the same phone number for the Robocall Mitigation Contact: 865-507-2025, and the RMD entries are attested as true, under penalty of perjury, by “VP” and “Vitaly Potapov.” For these reasons, this Notice refers to these entities collectively as “RSCoM.”

³ FCC, *FCC Issues Robocall Cease-and-Desist Letter to RSCoM*, <https://docs.fcc.gov/public/attachments/DOC-370915A1.pdf> (hereinafter “FCC’s Cease-and-Desist”).

⁴ FTC, *Warning Letter to RSCoM Ltd.*, https://www.ftc.gov/system/files/ftc_gov/pdf/pointofnoentry-rscomwarningletter.pdf (hereinafter “FTC’s Warning Letter”).

⁵ FCC’s Cease-and-Desist at 1.

⁶ FTC’s Warning Letter at 1–2.

During the course of its investigation of RSCoM, the Task Force requested the production of call detail records for all call traffic sent to and/or through your network or which you originated on behalf of your customers during a certain time period. Additionally, as noted in the 2023 Task Force Notice, as part of its investigation into the transmission of illegal robocalls and the providers and entities that originate and/or route them, the Task Force regularly reviews call traffic information from several industry sources, including USTelecom’s Industry Traceback Group (“ITG”)⁷ and ZipDX LLC (“ZipDX”)⁸.

Call traffic data from the ITG shows that it issued at least **997 traceback notices** to RSCoM since January 2019 for calls it accepted and/or transmitted onto and across the U.S. telephone network. These notices from the ITG cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning government imposters and impersonations, tax relief, private entity imposters, utilities disconnects, travel scams, student loan forgiveness, and others, with RSCoM identified as serving in various roles in the call path. At least **387 traceback notices** were issued since August 2022—after the Task Force issued its CID to RSCoM—and, of those, still more than **116 traceback notices** were issued since the 2023 Task Force Notice. Additionally, the traceback notices issued since August 2022 continue to show that RSCoM is being identified as the point-of-entry or gateway⁹ provider for this traffic, as well as the immediate downstream provider to the originating provider and the originating provider itself. Because the ITG estimates

⁷ Established in 2015, the ITG is a private collaborative industry group—composed of providers across wireline, wireless, VOIP, and cable services—that traces and identifies the sources of suspected illegal and suspicious robocalls. In December 2019, Congress enacted the Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) to combat the scourge of unlawful robocalls. *See* Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019). Following its enactment, the Federal Communications Commission designated the ITG as the official private-led traceback consortium charged with leading the voice communications industry’s efforts to trace the origin of suspected illegal robocalls through various communications networks through tracebacks. *See* 47 C.F.R. § 64.1203.

⁸ ZipDX is a provider of web- and phone-based collaboration services, which also focuses resources on developing and making technology available that is directed at mitigating illegal robocalls and other telephone-based fraud and abuse. ZipDX’s proprietary tool “RRAPTOR” is one such technology, which is an automated robocall surveillance tool that captures call recordings and information for calls largely associated with high-volume suspicious calling campaigns, and identifies the providers who have affixed their SHAKEN signatures to each of the captured calls, indicating that the provider is in the call path and whether those providers have attested to knowing the calling party who made the suspicious call and/or knowing of the calling party’s right to use that calling number to make that suspicious call. *See* ZipDX, What is RRAPTOR?, <https://legalcallsonly.org/what-is-rraptor/> (last visited Oct. 17, 2024).

⁹ *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, 87 FR 42916, 42917–18, para. 7 (2022) (defining a “gateway provider” as “a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider”).

that each traced call is representative of a large volume of similar illegal and/or suspicious calls,¹⁰ RSCoM is likely continuing to cause significant volumes of illegal and/or suspicious robocalls to ultimately reach U.S. consumers, despite traceback notifications from the ITG of this identified and suspected illegal call traffic.

Further, an analysis of a limited set of call detail records¹¹ from RSCoM's nationwide call traffic for a period between July 2021 and March 2022 shows that more than **10.275 million calls were made using invalid Caller ID numbers**, which means the calling numbers making the calls used a combination of numbers that were not assigned and/or recognized as valid by the North American Numbering Plan Administrator. Each call made using an invalid calling telephone number appears to have violated the Truth in Caller ID, 47 U.S.C. 227(e)(1) and 47 C.F.R. 64.1604(a), and the TCPA, 47 C.F.R. § 64.1200(n)(4)–(5).

Additionally, RSCoM's nationwide call traffic included more than **46,997 calls using illegally spoofed telephone numbers** for this same limited time period. The illegally spoofed calling numbers disguised calls as legitimate call traffic from local, state, and federal government agencies within the United States, and misrepresented callers' affiliations with law enforcement agencies and private sector entities. Each call made using an illegally spoofed calling telephone number appears to have violated the TSR, 16 C.F.R. § 310.4(a)(8), and the Truth in Caller ID: 47 U.S.C. § 227(e)(1) and 47 C.F.R. § 64.1604(a).

Finally, after an analysis of a subset of recorded voicemail messages that corresponded with the call detail records, more than **26,930 calls contained unlawful or fraudulent content**,

¹⁰ USTelecom, *Industry Traceback Group Policies and Procedures*, at 4 (last revised April 2022) (*ITG Policies & Procedures*) (defining "campaign" as "[a] group of calls with identical or nearly identical messaging as determined by the content and calling patterns of the caller," where "[a] single Campaign often represents hundreds of thousands or millions of calls"), *available at* <https://r01986.a2cdn1.secureserver.net/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf>.

¹¹ Call detail records or "CDRs" are automatically generated records of each attempted or completed call that reaches and/or crosses a voice service provider's network. CDRs generally include the following information:

- a. The date and time of the call attempt;
- b. The duration of the call (calls that fail to connect are generally denoted by a zero-second duration);
- c. The intended call recipient's telephone number;
- d. The originating or calling number from which the call was placed (which may be a real number or may be spoofed);
- e. An identifier such as a name or account number for the upstream provider that sent the call attempt to the provider's network; and
- f. An identifier for the downstream provider to which the provider attempts to route the call.

with each call's content appearing to have violated the TSR, 16 C.F.R. § 310.3(a)(2)(iii), and/or the TCPA, 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B), 47 C.F.R. § 64.1200(a)(2)–(3).

Information available from ZipDX indicates that RSCoM also attested to calls for a number of the same high-volume robocalling campaigns for which it received and/or continues to receive traceback notices from the ITG. For instance, during an eight-month period last year, ZipDX identified **116 suspicious calls** transmitted by RSCoM **from 46 unique calling numbers**,¹² exhibiting characteristics indicative of calls that are violations of federal and state laws; 100% of these calls were also made to numbers that have been registered on the National Do Not Call Registry.¹³ Additionally, about 70% of these calls were marked with a B-Level STIR/SHAKEN attestation, indicating that RSCoM knows the identities of the calling parties that originated these suspicious calls.

Lastly, analysis of a portion of RSCoM's likely involvement in the routing of nationwide call traffic concerning Amazon/Apple imposter robocalls was assessed. Between November 2020 and October 2024, among a nationwide sample of over 3.1 million transcribed and recorded Amazon/Apple imposter robocalls, **more than 189,700 of these Amazon/Apple imposter robocalls are estimated to be attributable to RSCoM**. Thus, of the more than 1.56 billion estimated Amazon/Apple imposter robocalls reaching consumers across the country in this sample during this period, **approximately 94.8 million of these scam robocalls are estimated to be attributable to RSCoM**.

A similar analysis of RSCoM's likely involvement in the routing of nationwide call traffic concerning SSA/IRS government imposter robocalls was assessed. Between July 2019 and June 2021, among a nationwide sample of over 3.8 million transcribed and recorded SSA/IRS government imposter robocalls, **more than 390,200 of these SSA/IRS government imposter robocalls are estimated to be attributable to RSCoM**. Thus, of the over 1.9 billion estimated SSA/IRS government imposter robocalls reaching consumers across the country in this sample during this period, **approximately 195.1 million of these scam robocalls are estimated to be attributable to RSCoM**.

¹² The use of many unique calling numbers for this volume of called numbers indicates a suspicious pattern in your call traffic of “snowshoeing” or “snowshoe spoofing,” which is a practice often employed by illegal robocallers and telemarketers to circumvent the protections of the STIR/SHAKEN call authentication framework by using significant quantities of unique numbers for caller IDs on a short-term or rotating basis in order to evade behavioral analytics detection, or to bypass or hinder call blocking or call labeling analytics based on the origination numbers. Telephone numbers used for snowshoeing sometimes cannot themselves receive incoming calls, which has the effect of impeding an audit of the legitimacy of these calling numbers.

¹³ Most calls captured by RRAPTOR are calls made to phone numbers that have been registered on the National Do Not Call Registry.

After reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force has concluded that RSCom is and/or has been involved in, at a minimum, transmitting call traffic indicative of, and associated with, recurrent high-volume illegal and/or suspicious robocalling campaigns and/or practices, which conduct could subject RSCom to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and state laws.

Overview of Select Relevant Laws

As RSCom well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,¹⁴ the Telephone Consumer Protection Act,¹⁵ and/or the Truth in Caller ID Act,¹⁶ as well as state consumer protection statutes.

Telemarketing Sales Rule (15 U.S.C. §§ 6101–6108; 16 C.F.R. Part 310)

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act which directed the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices.¹⁷ Pursuant to this directive, the FTC promulgated the Telemarketing Sales Rule (“TSR”). It is a violation of the TSR for voice service providers to provide substantial assistance to customers that the provider “knows or consciously avoids knowing” are engaged in practices that violate TSR provisions against deceptive and abusive telemarketing acts or practices.¹⁸ State Attorneys General have concurrent authority with the FTC to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR.¹⁹

Telephone Consumer Protection Act (47 U.S.C. § 227; 47 C.F.R. §§ 64.1200 and 64.1604)

Under the Telephone Consumer Protection Act (“TCPA”), the FCC promulgated rules restricting calls made with automated telephone dialing systems and calls delivering artificial or prerecorded voice messages.²⁰ Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.²¹ State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.²² The TCPA exempts from its prohibitions calls made for emergency

¹⁴ 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4.

¹⁵ 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

¹⁶ 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

¹⁷ 15 U.S.C. § 6102.

¹⁸ 16 C.F.R. § 310.3(b).

¹⁹ 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

²⁰ 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3).

²¹ 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2).

²² 47 U.S.C. § 227(g)(1).

purposes and certain other calls,²³ including those made with the “prior express consent” of the called party or with “prior express *written* consent” of the called party for telemarketing calls.²⁴ Note, however, the FCC has found in at least one instance that single consents purportedly given by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.²⁵

Truth in Caller ID Act (47 U.S.C. § 227(e))

Under the federal Truth in Caller ID Act, it is generally unlawful for a person to “knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.”²⁶ State Attorneys General have the authority to bring enforcement actions for violations of the Truth in Caller ID Act and its prohibition against illegal caller identification spoofing.²⁷ Such violative conduct can lead to assessments of civil penalties of up to \$10,000 for each violation, or three times that amount for each day of continuing

²³ 47 U.S.C. § 227(b)(1)(A)–(B), (b)(2)(B); 47 C.F.R. § 64.1200(a)(1)–(3), (a)(9).

²⁴ 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

²⁵ For example, in November 2022, the FCC issued an order requiring all voice service providers to block calls from provider Urth Access, LLC. In response to allegations concerning the transmission of illegal robocalls, Urth Access claimed to have obtained express consent for each of the calls. However, that consent stemmed from websites where consumers purportedly agreed to receive robocalls from over 5,000 “marketing partners” listed on a separate site. The FCC found this type of practice insufficient to constitute express consent to the marketing partners to contact the consumers. *See FCC Orders Voice Service Providers to Block Student Loan Robocalls*, <https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls> (Order); *FCC Issues Robocall Cease-and-Desist Letter to Urth Access*, <https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-urth-access> (Cease-and-Desist Letter). We note that this decision is consistent with the FTC’s interpretation of the express consent requirement of the TSR. *See* Federal Register, Vol. 73 No. 169, 2008 at 51182, <https://www.govinfo.gov/content/pkg/FR-2008-08-29/pdf/E8-20253.pdf> (consumer’s agreement with a seller to receive calls delivering prerecorded messages is nontransferable); *FTC, Complying with the Telemarketing Sales Rule, The Written Agreement Requirement*, <https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement>; *but see, Insurance Marketing Coalition, Ltd. v. Federal Communications Commission*, -- F.4th --, 2025 WL 289152 (11th Cir. 2025) (vacating and remanding FCC rule requiring those wishing to make a telemarketing or advertising robocall to obtain (1) consent from one called party to one seller at a time; and (2) consent that is logically and topically related to the interaction that prompted the consent).

²⁶ 47 U.S.C. § 227(e)(1); 47 C.F.R. § 64.1604.

²⁷ 47 U.S.C. § 227(e)(6).

violations.²⁸ Note that any penalties for violations of the Truth in Caller ID Act are in addition to those assessed for any other penalties provided for by the TCPA.²⁹

General Note regarding State Laws

In addition to their authority to enforce the above federal statutes, State Attorneys General are empowered to enforce their respective state laws regulating various aspects of the initiation and transmission of illegal robocall and telemarketing call traffic across the U.S. telephone network. Voice service providers transmitting calls into and throughout the states are obligated to familiarize themselves with, and abide by, all applicable state laws.

Requested Action in Response to this Notice

As noted above, the Task Force is providing this Notice in order to memorialize some of its investigative findings to date. The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, and has been, accepted and transmitted by and through RSCom's network, in order to ensure that your current business—and any subsequently-formed businesses—follow all applicable federal and state laws and regulations, including those referenced above. If subsequent investigation shows that RSCom and/or its principals continue to assist customers by initiating and/or transmitting call traffic not dissimilar from the traffic highlighted in this Notice, the Task Force may decide to pursue an enforcement action against RSCom, any later-formed business entities, and the principal owners and operators in common to both. Future action may also consist of referring the matter to the FCC for consideration of potential enforcement actions.³⁰

²⁸ 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

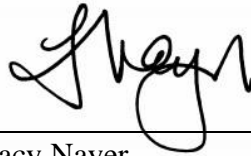
²⁹ *Id.*

³⁰ The FCC's authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter, *see, e.g., FCC Orders Avid Telecom to Cease and Desist Robocalls* <https://www.fcc.gov/document/fcc-orders-avid-telecom-cess-and-desist-robocalls> (issued Jun. 7, 2023); *FCC Issues Robocall Cease-and-Desist Letter to PZ/Illum*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-pzillum> (issued Oct. 21, 2021), a K4 Public Notice, *see FCC Enforcement Bureau Notifies All U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting From One Eye LLC*, <https://www.fcc.gov/document/fcc-takes-repeat-robocall-offenders-attempts-evade-enforcement> (issued Feb. 15, 2023), a Notice of Apparent Liability, *see, e.g., John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948 (2020), available at https://docs.fcc.gov/public/attachments/FCC-20-74A1_Rcd.pdf, a Consumer Communications Information Services Threat ("C-CIST") Designation Notice, *see FCC [Enforcement Bureau] Issues C-CIST Classification for "Royal Tiger"*, <https://www.fcc.gov/document/fcc-eb-issues-c-cist-classification-royal-tiger> (issued May 13, 2024), or proceedings that may result in removal from the Robocall Mitigation Database, *see, e.g., Viettel Business Solutions Company, Etihad*

For your information, we have informed several of our federal law enforcement counterparts—including our colleagues at the FCC’s Enforcement Bureau—of the Task Force’s intention to issue this Notice to RSCom. Finally, this Notice does not waive or otherwise preclude the Task Force from bringing an enforcement action related to conduct preceding the date of this Notice, including conduct that resulted in violations related to the call traffic referenced in this Notice.

The Task Force remains steadfast in its resolve to meaningfully curb illegal robocall traffic. Please direct any inquiries regarding this Notice to my attention at tnayer@ncdoj.gov.

Sincerely,



Tracy Nayer
Special Deputy Attorney General
Consumer Protection Division
North Carolina Department of Justice

Etisalat (Mobily), Claude ICT Poland Sp. z o. o. dba TeleCube.PL, Nervill LTD, Textodog Inc. dba Textodog and Textodog Software Inc., Phone GS, Computer Integrated Solutions dba CIS IT & Engineering, Datacom Specialists, DomainerSuite, Inc., Evernex SMC PVT LTD, Humbolt Voip, and My Taxi Ride Inc., Removal Order, 39 FCC Rcd 1319 (2024), available at <https://www.fcc.gov/document/fcc-removes-12-entities-robocall-mitigation-database>, the latter of which—if completed—would require all intermediate providers and terminating voice service providers to cease accepting your call traffic.

JEFF JACKSON
ATTORNEY GENERAL



TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL
TNAYER@NCDOJ.GOV

April 9, 2025

Oksana Grant, CEO
Global Net Holdings, Inc.
9813 Cowden Street
Philadelphia, PA 19115

Sent via certified mail, return receipt requested, and via email to oksana@globalnetholdings.net, lee@globalnetholdings.net, noc@globalnetholdings.net, info@globalnetholdings.net, sales@globalnetholdings.net, billing@globalnetholdings.net

Re: NOTICE from the Anti-Robocall Multistate Litigation Task Force Concerning Global Net Holdings, Inc.'s Involvement in Suspected Illegal Robocall Traffic

Dear Ms. Grant:

The Anti-Robocall Multistate Litigation Task Force's ("Task Force")¹ ongoing investigation of Global Net Holdings, Inc. ("Global Net Holdings")² has shown that Global Net Holdings has transmitted, and continues to transmit, suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is intended to apprise you of the Task Force's concerns regarding Global Net Holdings' call traffic, and to caution Global Net Holdings that it should scrutinize the call traffic of its current customers, evaluate the efficacy of its existing robocall mitigation policies, and cease transmitting illegal traffic on behalf of its current customers.

The Task Force requests that you take steps to prevent your network from continuing to be a source of apparently illegal robocalls. Transmission of these calls may be violations of the Telemarketing Sales Rule,³ the Telephone Consumer Protection Act,⁴ the Truth in Caller ID Act,⁵

¹ The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall ecosystem that are identified as being responsible for significant volumes of illegal and fraudulent robocall traffic routed into and across the country.

² Global Net Holdings, Inc.—FCC Registration No. 0019927979; Robocall Mitigation Database Nos. RMD0004139, RMD0009352—"Global Net Holdings") is reportedly a Pennsylvania corporation. In the FCC's Robocall Mitigation Database, Oksana Grant is listed as Global Net Holdings' Chief Executive Officer.

³ 15 U.S.C. §§ 6101-6108; 16 C.F.R. §§ 310.3, 310.4.

⁴ 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

⁵ 47 U.S.C. § 227(e); 47 C.F.R. § 64,1604.

as well as state consumer protection statutes. If, after receiving this Notice, Global Net Holdings continues to transmit calls for illegal robocall campaigns, the Task Force may decide to pursue an enforcement action against Global Net Holdings and its principal owners and/or operators.

Task Force’s Findings Regarding Global Net Holdings’ Call Traffic

As you are aware, on August 1, 2022, the Task Force issued its Civil Investigative Demand (“CID”) to Global Net Holdings to identify, investigate, and mitigate suspected illegal call traffic that is accepted onto, and transmitted across, Global Net Holdings’ network. Based on pertinent analyses and information available to the Task Force, it appears that Global Net Holdings is continuing to transmit calls associated with high-volume illegal and/or suspicious robocall campaigns.

As part of its investigation into the transmission of illegal robocalls and the providers and entities that originate and/or route them, the Task Force regularly reviews call traffic information from several industry sources, including USTelecom’s Industry Traceback Group (“ITG”)⁶ and ZipDX LLC (“ZipDX”).⁷

Call traffic data from the ITG shows that it issued at least **153 traceback notices** to Global Net Holdings since January 2019 for calls it accepted and/or transmitted onto and across the U.S. telephone network. These notices from the ITG cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning government and financial imposters and impersonations, Amazon suspicious charges, credit card interest rate reductions, Medicare scams, Chinese package delivery scams, cable discount scams, utility disconnect scams, and others, with

⁶ Established in 2015, the ITG is a private collaborative industry group—composed of providers across wireline, wireless, VOIP, and cable services—that traces and identifies the sources of suspected illegal and suspicious robocalls. In December 2019, Congress enacted the Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) to combat the scourge of unlawful robocalls. *See* Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019). Following its enactment, the Federal Communications Commission designated the ITG as the official private-led traceback consortium charged with leading the voice communications industry’s efforts to trace the origin of suspected illegal robocalls through various communications networks through tracebacks. *See* 47 C.F.R. § 64.1203.

⁷ ZipDX is a provider of web- and phone-based collaboration services, which also focuses resources on developing and making technology available that is directed at mitigating illegal robocalls and other telephone-based fraud and abuse. ZipDX’s proprietary tool “RRAPTOR” is one such technology, which is an automated robocall surveillance tool that captures call recordings and information for calls largely associated with high-volume suspicious calling campaigns, and identifies the providers who have affixed their SHAKEN signatures to each of the captured calls, indicating that the provider is in the call path and whether those providers have attested to knowing the calling party who made the suspicious call and/or knowing of the calling party’s right to use that calling number to make that suspicious call. *See* ZipDX, What is RRAPTOR?, <https://legalcallsonly.org/what-is-rraptor/> (last visited Oct. 17, 2024).

Global Net Holdings identified as serving primarily as the point-of-entry or gateway⁸ provider for most of this call traffic, and serving as the immediate downstream provider to the originating provider and as the originating provider itself for the remainder of this traffic. At least half of the traceback notices were sent to Global Net Holdings since August 2022, which is *after* the Task Force issued its CID to Global Net Holdings, and notices are still being issued in 2025. Because the ITG estimates that each traced call is representative of a large volume of similar illegal and/or suspicious calls,⁹ Global Net Holdings is likely causing significant volumes of illegal and/or suspicious robocalls to ultimately reach U.S. consumers, despite traceback notifications from the ITG of this identified and suspected illegal call traffic.

Further, ITG traceback data shows that Global Net Holdings reporting receiving illegal and/or suspicious robocalls directly from at least one foreign service provider not listed in the FCC’s Robocall Mitigation Database (“RMD”) at the time the calls were sent. ITG data shows that Global Net Holdings reported that calls were received from the foreign service provider edatelvoip.¹⁰ Providers may only accept calls directly from other domestic providers and foreign providers using U.S. telephone numbers in the caller ID field when those providers are listed in the RMD.¹¹ We note also that it appears Global Net Holdings has, in some instances, routed unauthenticated calls from foreign service providers while it was serving as a gateway provider in contravention of applicable rules and/or regulations.¹²

Information available from ZipDX indicates that Global Net Holdings also attested to calls for a number of the same high-volume robocalling campaigns for which it received and/or continues to receive traceback notices from the ITG. For instance, in the last year, ZipDX identified **355 suspicious calls** transmitted by Global Net Holdings **from 354 unique calling numbers**,¹³ exhibiting characteristics indicative of calls that are violations of federal and state

⁸ *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, 87 FR 42916, 42917–18, para. 7 (2022) (defining a “gateway provider” as “a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider”).

⁹ USTelecom, *Industry Traceback Group Policies and Procedures*, at 4 (last revised April 2022) (*ITG Policies & Procedures*) (defining “campaign” as “[a] group of calls with identical or nearly identical messaging as determined by the content and calling patterns of the caller,” where “[a] single Campaign often represents hundreds of thousands or millions of calls”), *available at* <https://r01986.a2cdn1.secureserver.net/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf>.

¹⁰ *See, e.g.*, ITG Traceback No. 19140.

¹¹ *See* 47 C.F.R. § 64.6305(g).

¹² *See* 47 C.F.R. § 64.6302(c); *see, e.g.*, ITG Traceback Nos. 24352, 24353.

¹³ The use of many unique calling numbers for this volume of called numbers indicates a suspicious pattern in your call traffic of “snowshoeing” or “snowshoe spoofing,” which is a practice often

laws; 94% of these calls were also made to numbers that have been registered on the National Do Not Call Registry.¹⁴ Additionally, about 35% of these calls were marked with a B-Level STIR/SHAKEN attestation, indicating that Global Net Holdings knows the identities of the calling parties that originated these suspicious calls.

Lastly, analysis of a portion of Global Net Holdings' likely involvement in the routing of nationwide call traffic concerning SSA government imposter robocalls was assessed. Between September 2020 and March 2021, among a nationwide sample of more than 937,700 transcribed and recorded SSA imposter robocalls, **approximately 59,833 of these SSA imposter robocalls are estimated to be attributable to Global Net Holdings.** Thus, of the over 468 million estimated SSA imposter robocalls reaching consumers across the country in this sample during this period, **approximately 29.9 million of these scam robocalls are estimated to be attributable to Global Net Holdings.**

After reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force has concluded that Global Net Holdings is and/or has been involved in, at a minimum, transmitting call traffic indicative of, and associated with, recurrent high-volume illegal and/or suspicious robocalling campaigns and/or practices, which conduct could subject Global Net Holdings to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and state laws.

Overview of Select Relevant Laws

As Global Net Holdings well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,¹⁵ the Telephone Consumer Protection Act,¹⁶ and/or the Truth in Caller ID Act,¹⁷ as well as state consumer protection statutes.

Telemarketing Sales Rule (15 U.S.C. §§ 6101–6108; 16 C.F.R. Part 310)

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act which directed the FTC to prescribe rules prohibiting deceptive telemarketing acts or

employed by illegal robocallers and telemarketers to circumvent the protections of the STIR/SHAKEN call authentication framework by using significant quantities of unique numbers for caller IDs on a short-term or rotating basis in order to evade behavioral analytics detection, or to bypass or hinder call blocking or call labeling analytics based on the origination numbers. Telephone numbers used for snowshoeing sometimes cannot themselves receive incoming calls, which has the effect of impeding an audit of the legitimacy of these calling numbers.

¹⁴ Most calls captured by RRAPTOR are calls made to phone numbers that have been registered on the National Do Not Call Registry.

¹⁵ 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4.

¹⁶ 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

¹⁷ 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

practices.¹⁸ Pursuant to this directive, the FTC promulgated the Telemarketing Sales Rule (“TSR”). It is a violation of the TSR for voice service providers to provide substantial assistance to customers that the provider “knows or consciously avoids knowing” are engaged in practices that violate TSR provisions against deceptive and abusive telemarketing acts or practices.¹⁹ State Attorneys General have concurrent authority with the FTC to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR.²⁰

Telephone Consumer Protection Act (47 U.S.C. § 227; 47 C.F.R. §§ 64.1200 and 64.1604)

Under the Telephone Consumer Protection Act (“TCPA”), the FCC promulgated rules restricting calls made with automated telephone dialing systems and calls delivering artificial or prerecorded voice messages.²¹ Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.²² State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.²³ The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,²⁴ including those made with the “prior express consent” of the called party or with “prior express *written* consent” of the called party for telemarketing calls.²⁵ Note, however, the FCC has found in at least one instance that single consents purportedly given by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.²⁶

¹⁸ 15 U.S.C. § 6102.

¹⁹ 16 C.F.R. § 310.3(b).

²⁰ 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

²¹ 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3).

²² 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2).

²³ 47 U.S.C. § 227(g)(1).

²⁴ 47 U.S.C. § 227(b)(1)(A)–(B), (b)(2)(B); 47 C.F.R. § 64.1200(a)(1)–(3), (a)(9).

²⁵ 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

²⁶ For example, in November 2022, the FCC issued an order requiring all voice service providers to block calls from provider Urth Access, LLC. In response to allegations concerning the transmission of illegal robocalls, Urth Access claimed to have obtained express consent for each of the calls. However, that consent stemmed from websites where consumers purportedly agreed to receive robocalls from over 5,000 “marketing partners” listed on a separate site. The FCC found this type of practice insufficient to constitute express consent to the marketing partners to contact the consumers. *See FCC Orders Voice Service Providers to Block Student Loan Robocalls*, <https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls> (Order); *FCC Issues Robocall Cease-and-Desist Letter to Urth Access*, <https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-urth-access> (Cease-and-Desist Letter). We note that this decision is consistent with the FTC’s interpretation of the express consent requirement of the TSR. *See* Federal Register, Vol. 73 No. 169, 2008 at 51182,

Truth in Caller ID Act (47 U.S.C. § 227(e))

Under the federal Truth in Caller ID Act, it is generally unlawful for a person to “knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.”²⁷ State Attorneys General have the authority to bring enforcement actions for violations of the Truth in Caller ID Act and its prohibition against illegal caller identification spoofing.²⁸ Such violative conduct can lead to assessments of civil penalties of up to \$10,000 for each violation, or three times that amount for each day of continuing violations.²⁹ Note that any penalties for violations of the Truth in Caller ID Act are in addition to those assessed for any other penalties provided for by the TCPA.³⁰

General Note regarding State Laws

In addition to their authority to enforce the above federal statutes, State Attorneys General are empowered to enforce their respective state laws regulating various aspects of the initiation and transmission of illegal robocall and telemarketing call traffic across the U.S. telephone network. Voice service providers transmitting calls into and throughout the states are obligated to familiarize themselves with, and abide by, all applicable state laws.

Requested Action in Response to this Notice

The Task Force is providing this Notice in order to memorialize some of its investigative findings to date. The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, and has been, accepted and transmitted by and through Global Net Holdings’ network, in order to ensure that your current business—and any subsequently-formed businesses—follow all applicable federal and state laws and regulations, including those referenced above. If subsequent investigation shows that Global Net Holdings and/or its principals continue to assist customers by initiating and/or transmitting call traffic not dissimilar from the traffic highlighted in this Notice, the Task Force may decide to pursue an enforcement action against Global Net Holdings, any later-formed business entities, and

<https://www.govinfo.gov/content/pkg/FR-2008-08-29/pdf/E8-20253.pdf> (consumer’s agreement with a seller to receive calls delivering prerecorded messages is nontransferable); *FTC, Complying with the Telemarketing Sales Rule, The Written Agreement Requirement*, <https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement>; *but see, Insurance Marketing Coalition, Ltd. v. Federal Communications Commission*, -- F.4th --, 2025 WL 289152 (11th Cir. 2025) (vacating and remanding FCC rule requiring those wishing to make a telemarketing or advertising robocall to obtain (1) consent from one called party to one seller at a time; and (2) consent that is logically and topically related to the interaction that prompted the consent).

²⁷ 47 U.S.C. § 227(e)(1); 47 C.F.R. § 64.1604.

²⁸ 47 U.S.C. § 227(e)(6).

²⁹ 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

³⁰ *Id.*

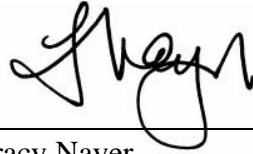
the principal owners and operators in common to both. Future action may also consist of referring the matter to the FCC for consideration of potential enforcement actions.³¹

For your information, we have informed several of our federal law enforcement counterparts—including our colleagues at the FCC’s Enforcement Bureau—of the Task Force’s intention to issue this Notice to Global Net Holdings. Finally, this Notice does not waive or otherwise preclude the Task Force from bringing an enforcement action related to conduct preceding the date of this Notice, including conduct that resulted in violations related to the call traffic referenced in this Notice.

³¹ The FCC’s authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter, *see, e.g., FCC Orders Avid Telecom to Cease and Desist Robocalls* <https://www.fcc.gov/document/fcc-orders-avid-telecom-cess-and-desist-robocalls> (issued Jun. 7, 2023); *FCC Issues Robocall Cease-and-Desist Letter to PZ/Illum*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-pzillum> (issued Oct. 21, 2021), a K4 Public Notice, *see FCC Enforcement Bureau Notifies All U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting From One Eye LLC*, <https://www.fcc.gov/document/fcc-takes-repeat-robocall-offenders-attempts-evade-enforcement> (issued Feb. 15, 2023), a Notice of Apparent Liability, *see, e.g., John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948 (2020), *available at* https://docs.fcc.gov/public/attachments/FCC-20-74A1_Rcd.pdf, a Consumer Communications Information Services Threat (“C-CIST”) Designation Notice, *see FCC [Enforcement Bureau] Issues C-CIST Classification for “Royal Tiger”*, <https://www.fcc.gov/document/fcc-eb-issues-c-cist-classification-royal-tiger> (issued May 13, 2024), or proceedings that may result in removal from the Robocall Mitigation Database, *see, e.g., Viettel Business Solutions Company, Etihad Etisalat (Mobily), Claude ICT Poland Sp. z o. o. dba TeleCube.PL, Nervill LTD, Textodog Inc. dba Textodog and Textodog Software Inc., Phone GS, Computer Integrated Solutions dba CIS IT & Engineering, Datacom Specialists, DomainerSuite, Inc., Evernex SMC PVT LTD, Humbolt Voip, and My Taxi Ride Inc.*, Removal Order, 39 FCC Rcd 1319 (2024), *available at* <https://www.fcc.gov/document/fcc-removes-12-entities-robocall-mitigation-database>, the latter of which—if completed—would require all intermediate providers and terminating voice service providers to cease accepting your call traffic.

The Task Force remains steadfast in its resolve to meaningfully curb illegal robocall traffic. Please direct any inquiries regarding this Notice to my attention at tnayer@ncdoj.gov.

Sincerely,

A handwritten signature in black ink, appearing to read 'Tracy Nayer', is positioned above a horizontal line.

Tracy Nayer
Special Deputy Attorney General
Consumer Protection Division
North Carolina Department of Justice

JEFF JACKSON
ATTORNEY GENERAL



TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL
TNAYER@NCDOJ.GOV

April 9, 2025

Michael Moran, CEO and President
thinQ Technologies, Inc. dba Commio and Teli Communications, LLC
c/o Spencer Wiles
Robinson Bradshaw
101 N. Tryon Street, Suite 1900
Charlotte, NC 28246

*Sent via certified mail, return receipt requested, and via email to
SWiles@robinsonbradshaw.com*

Re: SECOND AND FINAL NOTICE LETTER from the Anti-Robocall Multistate Litigation Task Force Concerning thinQ Technologies, Inc. dba Commio and Teli Communications, LLC's Continued Involvement in Suspected Illegal Robocall Traffic

Dear Mr. Moran:

The Anti-Robocall Multistate Litigation Task Force's ("Task Force")¹ investigation of thinQ Technologies, Inc. dba Commio and Teli Communications, LLC—"thinQ/Commio"² has shown that thinQ/Commio has transmitted, and continues to transmit, suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is the Task Force's second and final attempt to informally apprise you of the Task Force's concerns regarding thinQ/Commio call traffic, and to caution thinQ/Commio that it should scrutinize the call traffic of its current customers, evaluate the efficacy of its existing robocall mitigation policies, and cease transmitting illegal traffic on behalf of its current customers.

¹ The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall ecosystem that are identified as being responsible for significant volumes of illegal and fraudulent robocall traffic routed into and across the country.

² thinQ Technologies, Inc. dba Commio and Teli Communications, LLC—FCC Registration Nos. 0028135630, 0021852504, 0025309758; Robocall Mitigation Database No. RMD0005575—"thinQ/Commio" is a foreign corporation registered in North Carolina. Michael Moran is identified as thinQ/Commio's Chief Executive Officer and President. Kristen Broome is thinQ/Commio's Chief Financial Officer.

The Task Force provides this Notice in order to memorialize some of its investigative findings to date.

Task Force’s Findings Regarding thinQ/Commio’s Call Traffic

As you are aware, on March 22, 2022, thinQ/Commio was issued a Cease-and-Desist Notice³ from the Federal Communications Commission (“FCC”). The FCC’s Cease-and-Desist provided that thinQ/Commio was “apparently originating and transmitting illegal robocall traffic on behalf of one or more of its clients” for “multiple illegal robocall campaigns.”⁴ The FCC’s Cease-and-Desist referenced applicable federal laws and rules, and thinQ/Commio’s legal obligations under the same.

On August 1, 2022, the Task Force issued its Civil Investigative Demand (“CID”) to thinQ/Commio to identify, investigate, and mitigate suspected illegal call traffic that is or was accepted onto, and transmitted across, thinQ/Commio’s network. On November 3, 2023, the Task Force issued a Notice to thinQ/Commio (“2023 Task Force Notice”) memorializing some of the Task Force’s findings concerning thinQ/Commio’s call traffic, informing you of the Task Force’s continuing concerns regarding your call traffic, and cautioning thinQ/Commio that it should cease transmitting any illegal traffic immediately. Based on pertinent analyses and information available to the Task Force, it appears that thinQ/Commio has continued to transmit calls associated with high-volume illegal and/or suspicious robocall campaigns.

During the course of its investigation of thinQ/Commio, the Task Force requested the production of call detail records for all call traffic sent to and/or through your network or which you originated on behalf of your customers during a certain time period. Additionally, as noted in the 2023 Task Force Notice, as part of its investigation into the transmission of illegal robocalls and the providers and entities that originate and/or route them, the Task Force regularly reviews call traffic information from several industry sources, including USTelecom’s Industry Traceback

³ FCC, *FCC Issues Robocall Cease-and-Desist Letter to thinQ*, <https://docs.fcc.gov/public/attachments/DOC-381498A1.pdf> (hereinafter “FCC’s Cease-and-Desist”).

⁴ FCC’s Cease-and-Desist at 1.

Group (“ITG”)⁵ and ZipDX LLC (“ZipDX”)⁶.

Call traffic data from the ITG shows that it issued at least **511 traceback notices** to thinQ/Commio since January 2019 for calls it accepted and/or transmitted onto and across the U.S. telephone network. These notices from the ITG cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning government imposters and impersonations, debt relief/financing, utilities, loan approvals, Amazon suspicious charges, student loan forgiveness, DirecTV discounts, sweepstakes, and others, with thinQ/Commio identified as serving in various roles in the call path. At least **283 traceback notices** were issued since August 2022—after the Task Force issued its CID to thinQ/Commio—and, of those, still more than **128 traceback notices** were issued since the 2023 Task Force Notice. While the traceback notices issued since August 2022 show that thinQ/Commio is not as frequently identified as the point-of-entry or gateway⁷ provider for this traffic, thinQ/Commio is still regularly identified as the immediate downstream provider to the originating provider or the originating provider itself for at least half of this traffic. Because the ITG estimates that each traced call is representative of a large volume of similar illegal and/or suspicious calls,⁸ thinQ/Commio is likely continuing to cause significant volumes of illegal

⁵ Established in 2015, the ITG is a private collaborative industry group—composed of providers across wireline, wireless, VOIP, and cable services—that traces and identifies the sources of suspected illegal and suspicious robocalls. In December 2019, Congress enacted the Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) to combat the scourge of unlawful robocalls. *See* Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019). Following its enactment, the Federal Communications Commission designated the ITG as the official private-led traceback consortium charged with leading the voice communications industry’s efforts to trace the origin of suspected illegal robocalls through various communications networks through tracebacks. *See* 47 C.F.R. § 64.1203.

⁶ ZipDX is a provider of web- and phone-based collaboration services, which also focuses resources on developing and making technology available that is directed at mitigating illegal robocalls and other telephone-based fraud and abuse. ZipDX’s proprietary tool “RRAPTOR” is one such technology, which is an automated robocall surveillance tool that captures call recordings and information for calls largely associated with high-volume suspicious calling campaigns, and identifies the providers who have affixed their SHAKEN signatures to each of the captured calls, indicating that the provider is in the call path and whether those providers have attested to knowing the calling party who made the suspicious call and/or knowing of the calling party’s right to use that calling number to make that suspicious call. *See* ZipDX, What is RRAPTOR?, <https://legalcallsonly.org/what-is-rraptor/> (last visited Oct. 17, 2024).

⁷ *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, 87 FR 42916, 42917–18, para. 7 (2022) (defining a “gateway provider” as “a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider”).

⁸ USTelecom, *Industry Traceback Group Policies and Procedures*, at 4 (last revised April 2022) (*ITG Policies & Procedures*) (defining “campaign” as “[a] group of calls with identical or nearly

and/or suspicious robocalls to ultimately reach U.S. consumers, despite traceback notifications from the ITG of this identified and suspected illegal call traffic.

Further, an analysis of a limited set of call detail records⁹ from thinQ/Commio's nationwide call traffic for a period of just over six months between March 2022 and mid-September 2022 shows that more than **114.3 million calls were made using invalid Caller ID numbers**, which means the calling numbers making the calls used a combination of numbers that were not assigned and/or recognized as valid by the North American Numbering Plan Administrator. Each call made using an invalid calling telephone number appears to have violated the Truth in Caller ID, 47 U.S.C. 227(e)(1) and 47 C.F.R. 64.1604(a), and the TCPA, 47 C.F.R. § 64.1200(n)(4)–(5).

Additionally, thinQ/Commio's nationwide call traffic included more than **281,480 calls using illegally spoofed telephone numbers** for this same limited time period. The illegally spoofed calling numbers disguised calls as legitimate call traffic from local, state, and federal government agencies within the United States, and misrepresented callers' affiliations with law enforcement agencies and private sector entities. Each call made using an illegally spoofed calling telephone number appears to have violated the TSR, 16 C.F.R. § 310.4(a)(8), and the Truth in Caller ID: 47 U.S.C. § 227(e)(1) and 47 C.F.R. § 64.1604(a).

Finally, after an analysis of a subset of recorded voicemail messages that corresponded with the call detail records, more than **209,800 calls contained unlawful or fraudulent content**, with each call's content appearing to have violated the TSR, 16 C.F.R. § 310.3(a)(2)(iii), and/or the TCPA, 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B), 47 C.F.R. § 64.1200(a)(2)–(3).

Information available from ZipDX indicates that thinQ/Commio also attested to calls for a number of the same high-volume robocalling campaigns for which it received and/or continues to

identical messaging as determined by the content and calling patterns of the caller," where "[a] single Campaign often represents hundreds of thousands or millions of calls"), *available at* <https://r01986.a2cdn1.secureserver.net/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf>.

⁹ Call detail records or "CDRs" are automatically generated records of each attempted or completed call that reaches and/or crosses a voice service provider's network. CDRs generally include the following information:

- a. The date and time of the call attempt;
- b. The duration of the call (calls that fail to connect are generally denoted by a zero-second duration);
- c. The intended call recipient's telephone number;
- d. The originating or calling number from which the call was placed (which may be a real number or may be spoofed);
- e. An identifier such as a name or account number for the upstream provider that sent the call attempt to the provider's network; and
- f. An identifier for the downstream provider to which the provider attempts to route the call.

receive traceback notices from the ITG. For instance, in just the last several months, ZipDX identified **1,960 suspicious calls** transmitted by thinQ/Commio **from 1,159 unique calling numbers**,¹⁰ exhibiting characteristics indicative of calls that are violations of federal and state laws; 87% of these calls were also made to numbers that have been registered on the National Do Not Call Registry.¹¹ Additionally, 33% of these calls were marked with an A-Level STIR/SHAKEN attestation, indicating that thinQ/Commio both knows the identities of the calling parties that originated these suspicious calls and knows that those callers have legitimately acquired volumes of numbering resources that are being used to make these calls, while 63% of these calls were marked with a B-Level STIR/SHAKEN attestation, indicating that thinQ/Commio, at a minimum, knows the identities of the calling parties that originated these suspicious calls.

Lastly, analysis of a portion of thinQ/Commio's likely involvement in the routing of nationwide call traffic concerning Amazon/Apple imposter robocalls was assessed. Between March 2022 and March 2023, among a nationwide sample of over 953,000 transcribed and recorded Amazon/Apple imposter robocalls, **approximately 29,640 of these Amazon/Apple imposter robocalls are estimated to be attributable to thinQ/Commio**. Thus, of the more than 476 million estimated Amazon/Apple imposter robocalls reaching consumers across the country in this sample during this period, **approximately 14.8 million of these scam robocalls are estimated to be attributable to thinQ/Commio**.

A similar analysis of thinQ/Commio's likely involvement in the routing of nationwide call traffic concerning SSA imposter robocalls was assessed. During the three-month period between July 2021 and September 2021, among a nationwide sample of over 400,000 transcribed and recorded SSA imposter robocalls, **approximately 39,096 of these SSA imposter robocalls are estimated to be attributable to thinQ/Commio**. Thus, of the over 200 million estimated SSA imposter robocalls reaching consumers across the country in this sample during this limited period, **approximately 19.5 million of these scam robocalls are estimated to be attributable to thinQ/Commio**.

In addition, we noted at least two instances in which thinQ/Commio identified a non-provider entity as its upstream voice service provider customer in the call path.¹² When a

¹⁰ The use of many unique calling numbers for this volume of called numbers indicates a suspicious pattern in your call traffic of "snowshoeing" or "snowshoe spoofing," which is a practice often employed by illegal robocallers and telemarketers to circumvent the protections of the STIR/SHAKEN call authentication framework by using significant quantities of unique numbers for caller IDs on a short-term or rotating basis in order to evade behavioral analytics detection, or to bypass or hinder call blocking or call labeling analytics based on the origination numbers. Telephone numbers used for snowshoeing sometimes cannot themselves receive incoming calls, which has the effect of impeding an audit of the legitimacy of these calling numbers.

¹¹ Most calls captured by RRAPTOR are calls made to phone numbers that have been registered on the National Do Not Call Registry.

¹² See, e.g., ITG Traceback Nos. 18162, 18163.

non-provider upstream customer transmits a call to thinQ/Commio, thinQ/Commio must identify itself as the originating provider in the call path.¹³

After reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force has concluded that thinQ/Commio is and/or has been involved in, at a minimum, transmitting call traffic indicative of, and associated with, recurrent high-volume illegal and/or suspicious robocalling campaigns and/or practices, which conduct could subject thinQ/Commio to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and state laws.

Overview of Select Relevant Laws

As thinQ/Commio well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,¹⁴ the Telephone Consumer Protection Act,¹⁵ and/or the Truth in Caller ID Act,¹⁶ as well as state consumer protection statutes.

Telemarketing Sales Rule (15 U.S.C. §§ 6101–6108; 16 C.F.R. Part 310)

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act which directed the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices.¹⁷ Pursuant to this directive, the FTC promulgated the Telemarketing Sales Rule (“TSR”). It is a violation of the TSR for voice service providers to provide substantial assistance to customers that the provider “knows or consciously avoids knowing” are engaged in practices that violate TSR provisions against deceptive and abusive telemarketing acts or practices.¹⁸ State Attorneys General have concurrent authority with the FTC to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR.¹⁹

Telephone Consumer Protection Act (47 U.S.C. § 227; 47 C.F.R. §§ 64.1200 and 64.1604)

Under the Telephone Consumer Protection Act (“TCPA”), the FCC promulgated rules restricting calls made with automated telephone dialing systems and calls delivering artificial or prerecorded voice messages.²⁰ Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.²¹ State Attorneys General are authorized to

¹³ See 47 C.F.R. § 64.6301(a)(2).

¹⁴ 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4.

¹⁵ 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

¹⁶ 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

¹⁷ 15 U.S.C. § 6102.

¹⁸ 16 C.F.R. § 310.3(b).

¹⁹ 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

²⁰ 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3).

²¹ 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2).

bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.²² The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,²³ including those made with the “prior express consent” of the called party or with “prior express *written* consent” of the called party for telemarketing calls.²⁴ Note, however, the FCC has found in at least one instance that single consents purportedly given by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.²⁵

Truth in Caller ID Act (47 U.S.C. § 227(e))

Under the federal Truth in Caller ID Act, it is generally unlawful for a person to “knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.”²⁶ State Attorneys General have the authority to bring enforcement actions for violations of the Truth in Caller ID Act and its prohibition against illegal caller identification spoofing.²⁷ Such violative conduct can lead to assessments of civil penalties of up to \$10,000 for each violation, or three times that amount for each day of continuing

²² 47 U.S.C. § 227(g)(1).

²³ 47 U.S.C. § 227(b)(1)(A)–(B), (b)(2)(B); 47 C.F.R. § 64.1200(a)(1)–(3), (a)(9).

²⁴ 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

²⁵ For example, in November 2022, the FCC issued an order requiring all voice service providers to block calls from provider Urth Access, LLC. In response to allegations concerning the transmission of illegal robocalls, Urth Access claimed to have obtained express consent for each of the calls. However, that consent stemmed from websites where consumers purportedly agreed to receive robocalls from over 5,000 “marketing partners” listed on a separate site. The FCC found this type of practice insufficient to constitute express consent to the marketing partners to contact the consumers. *See FCC Orders Voice Service Providers to Block Student Loan Robocalls*, <https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls> (Order); *FCC Issues Robocall Cease-and-Desist Letter to Urth Access*, <https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-urth-access> (Cease-and-Desist Letter). We note that this decision is consistent with the FTC’s interpretation of the express consent requirement of the TSR. *See* Federal Register, Vol. 73 No. 169, 2008 at 51182, <https://www.govinfo.gov/content/pkg/FR-2008-08-29/pdf/E8-20253.pdf> (consumer’s agreement with a seller to receive calls delivering prerecorded messages is nontransferable); *FTC, Complying with the Telemarketing Sales Rule, The Written Agreement Requirement*, <https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement>; *but see, Insurance Marketing Coalition, Ltd. v. Federal Communications Commission*, -- F.4th --, 2025 WL 289152 (11th Cir. 2025) (vacating and remanding FCC rule requiring those wishing to make a telemarketing or advertising robocall to obtain (1) consent from one called party to one seller at a time; and (2) consent that is logically and topically related to the interaction that prompted the consent).

²⁶ 47 U.S.C. § 227(e)(1); 47 C.F.R. § 64.1604.

²⁷ 47 U.S.C. § 227(e)(6).

violations.²⁸ Note that any penalties for violations of the Truth in Caller ID Act are in addition to those assessed for any other penalties provided for by the TCPA.²⁹

General Note regarding State Laws

In addition to their authority to enforce the above federal statutes, State Attorneys General are empowered to enforce their respective state laws regulating various aspects of the initiation and transmission of illegal robocall and telemarketing call traffic across the U.S. telephone network. Voice service providers transmitting calls into and throughout the states are obligated to familiarize themselves with, and abide by, all applicable state laws.

Requested Action in Response to this Notice

As noted above, the Task Force is providing this Notice in order to memorialize some of its investigative findings to date. The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, and has been, accepted and transmitted by and through thinQ/Commio's network, in order to ensure that your current business—and any subsequently-formed businesses—follow all applicable federal and state laws and regulations, including those referenced above. If subsequent investigation shows that thinQ/Commio and/or its principals continue to assist customers by initiating and/or transmitting call traffic not dissimilar from the traffic highlighted in this Notice, the Task Force may decide to pursue an enforcement action against thinQ/Commio, any later-formed business entities, and the principal owners and operators in common to both. Future action may also consist of referring the matter to the FCC for consideration of potential enforcement actions.³⁰

²⁸ 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

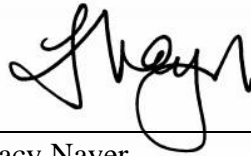
²⁹ *Id.*

³⁰ The FCC's authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter, *see, e.g., FCC Orders Avid Telecom to Cease and Desist Robocalls* <https://www.fcc.gov/document/fcc-orders-avid-telecom-cess-and-desist-robocalls> (issued Jun. 7, 2023); *FCC Issues Robocall Cease-and-Desist Letter to PZ/Illum*, <https://www.fcc.gov/document/fcc-issues-robocall-cess-and-desist-letter-pzillum> (issued Oct. 21, 2021), a K4 Public Notice, *see FCC Enforcement Bureau Notifies All U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting From One Eye LLC*, <https://www.fcc.gov/document/fcc-takes-repeat-robocall-offenders-attempts-evade-enforcement> (issued Feb. 15, 2023), a Notice of Apparent Liability, *see, e.g., John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948 (2020), available at https://docs.fcc.gov/public/attachments/FCC-20-74A1_Rcd.pdf, a Consumer Communications Information Services Threat (“C-CIST”) Designation Notice, *see FCC [Enforcement Bureau] Issues C-CIST Classification for “Royal Tiger”*, <https://www.fcc.gov/document/fcc-eb-issues-c-cist-classification-royal-tiger> (issued May 13, 2024), or proceedings that may result in removal from the Robocall Mitigation Database, *see, e.g., Viettel Business Solutions Company, Etihad*

For your information, we have informed several of our federal law enforcement counterparts—including our colleagues at the FCC’s Enforcement Bureau—of the Task Force’s intention to issue this Notice to thinQ/Commio. Finally, this Notice does not waive or otherwise preclude the Task Force from bringing an enforcement action related to conduct preceding the date of this Notice, including conduct that resulted in violations related to the call traffic referenced in this Notice.

The Task Force remains steadfast in its resolve to meaningfully curb illegal robocall traffic. Please direct any inquiries regarding this Notice to my attention at tnayer@ncdoj.gov.

Sincerely,



Tracy Nayer
Special Deputy Attorney General
Consumer Protection Division
North Carolina Department of Justice

Etisalat (Mobily), Claude ICT Poland Sp. z o. o. dba TeleCube.PL, Nervill LTD, Textodog Inc. dba Textodog and Textodog Software Inc., Phone GS, Computer Integrated Solutions dba CIS IT & Engineering, Datacom Specialists, DomainerSuite, Inc., Evernex SMC PVT LTD, Humbolt Voip, and My Taxi Ride Inc., Removal Order, 39 FCC Rcd 1319 (2024), available at <https://www.fcc.gov/document/fcc-removes-12-entities-robocall-mitigation-database>, the latter of which—if completed—would require all intermediate providers and terminating voice service providers to cease accepting your call traffic.