

JEFF JACKSON
ATTORNEY GENERAL



TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL
TNAYER@NCDOJ.GOV

December 3, 2025

Bandwidth, Inc.
Greg Rogers, Head of Global Policy and Regulatory Affairs
Emily Harlan, Sr. VP, Legal
Stephen Thayer, Director, Fraud Operations
2230 Bandmate Way
Raleigh, N.C. 27607

Sent via certified mail, return receipt requested, and via email to sthayer@bandwidth.com; charlan@bandwidth.com; grogers@bandwidth.com

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

Dear Messrs. Rogers and Thayer and Ms. Harlan:

The Anti-Robocall Multistate Litigation Task Force's ("Task Force")¹ ongoing investigation of Bandwidth, Inc. ("Bandwidth")² has shown that Bandwidth has transmitted—and continues to transmit—calls associated with high-volume illegal and/or suspicious robocall campaigns on behalf of one or more of its customers. This Notice is intended to apprise you of the Task Force's concerns regarding Bandwidth's call traffic, and to caution Bandwidth that it should scrutinize the call traffic of its current customers, evaluate the efficacy of its existing robocall mitigation plan and policies, Know-Your-Customer, and onboarding practices, and cease transmitting illegal traffic on behalf of its current customers.

While we have appreciated Bandwidth's willingness to this point to engage in conversations with the Task Force about our concerns regarding its call traffic, because our concerns linger, and for your edification, 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 FCC Registration No. 0015443773; Robocall Mitigation Database No. RMD0002564.

Task Force's Findings and Concerns Regarding Bandwidth's Call Traffic

As Bandwidth well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule (“the TSR”),³ the Telephone Consumer Protection Act (“the TCPA”),⁴ and/or the Truth in Caller ID Act,⁵ as well as state consumer protection statutes. State Attorneys General are authorized to bring enforcement actions under these federal statutes and rules.⁶ State Attorneys General are also 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.

As part of its investigation into the transmission of illegal robocalls and the providers and entities that originate and/or transmit them, the Task Force regularly reviews call traffic information from several industry sources, including USTelecom's Industry Traceback Group

³ 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4. It is a violation of the Federal Trade Commission's 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. 16 C.F.R. § 310.3(b).

⁴ 47 U.S.C. § 227; 47 C.F.R. §§ 64.1200, 64.1604. Under the TCPA, the Federal Communications Commission promulgated rules restricting calls made with automated telephone dialing systems, calls delivering artificial or prerecorded voice messages, 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3), and generally prohibiting solicitation calls placed to numbers on the National Do Not Call Registry. 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2). The TCPA also restricts all artificial or prerecorded voice messages that fail to disclose the identity and telephone number of the caller responsible for initiating the call and that fail to provide an automated opt-out mechanism in advertising or telemarketing messages. 47 U.S.C. § 227(d)(3) and 47 C.F.R. § 64.1200(b).

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

⁶ State Attorneys General have concurrent authority with the Federal Trade Commission to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR. 15 U.S.C. § 6103; 16 C.F.R. § 310.7. State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA. 47 U.S.C. § 227(g)(1). 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, 47 U.S.C. § 227(e)(6), which 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, and which penalties are assessed in addition to those for any other penalties provided for by the TCPA. 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

(“ITG”)⁷ and ZipDX LLC (“ZipDX”).⁸

Call traffic data from the ITG shows that it issued at least **3,060 traceback notices** to Bandwidth 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 Amazon/Apple imposters, SSA/IRS government imposters, financial services/order imposters, auto warranty scams, credit card interest rate and debt reduction scams, cable and utility discount scams, Medicare and health insurance scams, law enforcement imposters, Chinese language-based scams, mortgage scams, sweepstakes scams, COVID-related scams, home improvement scams, student loan scams, tech support scams, and others, with Bandwidth identified as the point-of-entry or gateway⁹ provider or as the immediate downstream provider to the originating provider for more than 24% of this traffic. At least **2,319 of those traceback notices** were sent to Bandwidth since August 2022, which is *after* the Task Force first reached out about its concerns regarding Bandwidth’s call traffic, 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,¹⁰ Bandwidth is likely causing significant

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. 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 Nov. 29, 2025).

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”).

¹⁰ USTelecom, *Industry Traceback Group Policies and Procedures*, at 13 (last revised August 2025) (*ITG Policies & Procedures*) (defining “campaign” as “[a] group of potentially hundreds of

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.

More recently, since July 2025, Bandwidth has been issued at least 487 tracebacks, with Bandwidth identified as the gateway provider or as the immediate downstream provider to the originating provider for more than 34% of recurrent high-volume illegal and/or suspicious robocalling campaigns including Amazon and other brand imposters and financial impersonations.

Bandwidth accepted and transmitted this recent call traffic directly from the following voice service providers that were identified as having originated these illegal and/or suspicious robocalls:

- Active Solutions Group
- Altaworx LLC
- AMCS LLC / Amazon Chime / Amazon Connect Cloud Contact Center
- Anveo, Inc.
- BCM One Cloud Communications LLC dba Flowroute / SIP.US
- BrightArrow Technologies, Inc.
- Broadband Dynamics, LLC.
- Bulk Solutions
- California Telecom, Inc.
- CallCurrent, Inc. / dba MightyCall / dba Omnivoice
- CallFire, Inc. / dba EZ Texting
- CMSInter.Net LLC
- Comm Suite LLC
- CoreDial, LLC
- Crosstel Tandem, Inc.
- Dialpad
- Filippo Justice Inc dba Blink Voice
- FluentStream Technologies, LLC
- Google
- IDT Telecom
- LogMeIn / GoTo Communications, Inc
- Matrix Telecom LLC / dba Vartec Telecom / Lingo Management LLC
- Momentum Telecom, Inc
- MyTelepath Inc.
- Premier IT Networks Inc
- PULSAR360 Corp.
- QuestBlue Systems Inc.
- Ring Central, Inc.
- Sangoma US Inc.

thousands or more calls with identical or nearly identical messaging, as determined by the content and calling patterns of the calls”), available at https://tracebacks.org/wp-content/uploads/2025/09/ITG_Policies-Procedures_Aug_2025.pdf.

- Sparkplug IP, LLC
- Stimulus Technologies of California, LLC
- T-Mobile USA, Inc. / USCellular
- Telengy LLC / Callcentric
- Telnyx
- Turkana, LLC
- Unified Global Solutions, LLC
- Veracity Networks, LLC
- Versatel LLC dba 46 Labs Communicati
- Verve Cloud, Inc.
- Victory Telecom, Inc.
- Viirtue LLC
- VirtualPBX.com, Inc
- VOIP Street / VoIP Innovations
- Vonage
- Zella Technologies, LLC

Bandwidth also accepted this illegal and/or suspicious robocalls onto the U.S. telephone network directly from the following foreign voice service providers:

- 9171-5573 Quebec Inc dba VoIP.ms / Swiftvox
- Hayyul Communications
- SherWeb Inc
- Viva Communications / Pennytel Ltd

Bandwidth then transmitted this illegal and/or suspicious call traffic directly to the following providers:

- All Access Telecom
- ANI Networks / NOS / Affinity Network, Inc.
- AT&T
- Brightlink /NUSO LLC / SoTel Systems / VoIPLink
- Centurylink / Lumen / Qwest / Level3
- Comcast
- Computertel, Inc. / Talktel Directo
- HFA Services LLC dba Call48
- Peerless Network / Airus / Infobip
- Sinch / Inteliquent / Onvoy / Vitelity / Neutral Tandem
- Skye Telecom LLC
- T-Mobile USA, Inc. / USCellular
- Verizon

Further, analysis of a portion of Bandwidth’s likely involvement in the routing of nationwide call traffic concerning Amazon/Apple imposter robocalls was assessed. Between October 2021 and November 2024, among a nationwide sample of approximately 2 million transcribed and recorded Amazon/Apple imposter robocalls, **over 325,500 of these Amazon/Apple imposter robocalls were estimated to be facilitated by Bandwidth.** Thus, of the over 1 billion estimated Amazon/Apple imposter robocalls reaching consumers across the country in this sample during this period, **approximately 162.7 million of these scam robocalls were estimated to be facilitated by Bandwidth.**

A similar analysis of Bandwidth’s likely involvement in the routing of nationwide call traffic concerning SSA/IRS government imposter robocalls was assessed. Between May 2020 and April 2024, among a nationwide sample of approximately 5.7 million transcribed and recorded SSA/IRS government imposter robocalls, **more than 602,000 of these SSA/IRS government imposter robocalls were estimated to be facilitated by Bandwidth.** Thus, of the over 2.87 billion estimated SSA/IRS government imposter robocalls reaching consumers across the country in this sample during this period, **approximately 301 million of these scam robocalls were estimated to be facilitated by Bandwidth.**

Additionally, between July 2020 and November 2024, 14% of all ITG tracebacks related to financial services/order imposter robocalls were facilitated by Bandwidth. In December 2024 alone, **14% of all tracebacks related to financial services/order imposter robocalls were facilitated by Bandwidth,** indicating no material change from the multi-year average of financial services/order imposter robocalls facilitated by Bandwidth despite its continual awareness of the same provided by servicing **at least 521 tracebacks overall that were related to financial services/order imposter robocalls.**

Finally, information available from ZipDX indicates that Bandwidth 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 12 months, ZipDX identified more than **1,306 suspicious calls** transmitted by Bandwidth **from 704 unique calling numbers**,¹¹ exhibiting characteristics indicative of calls that are violations of federal and state laws; more than 97% of these calls were also made to numbers that have been registered on the National Do Not Call Registry.¹² Additionally, more than 55% of these calls were marked with an “A” or “B” attestation, indicating that Bandwidth either knows the identities of the calling parties that originated these suspicious calls and knows that those callers have legitimately

¹¹ 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.

¹² Most calls captured by RRAPTOR are calls made to phone numbers that have been registered on the National Do Not Call Registry.

acquired volumes of numbering resources that are being used to make these suspicious calls (“A” attestation), or, at a minimum, knows the identities of the calling parties that originated these suspicious calls (“B” attestation).

While we understand that, because of the volume of traffic it transmits, Bandwidth is differently positioned in the ecosystem than smaller providers that serve primarily as intermediate providers, the Task Force believes that precisely because of Bandwidth's position, prominence, and dominance in this space, Bandwidth is better positioned to do more—and should do more—to reevaluate its choice to accept call traffic from recurring bad actors, either directly or indirectly, in order to meaningfully mitigate the identified and suspected illegal call traffic that those bad actors are being permitted to route across the U.S. telephone network with Bandwidth's help.

Thus, after reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force has concluded that Bandwidth 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 Bandwidth to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and 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 customers that are regularly using Bandwidth's network to originate and/or transmit route suspected illegal call traffic.

The Task Force requests that you provide us with a response within 35 days of the issuance of this Notice detailing how Bandwidth intends to address the concerns identified herein.

As a matter of courtesy, we have informed several of our federal law enforcement counterparts—including our colleagues at the FCC's Enforcement Bureau¹³—of the Task Force's intention to issue this Notice.

¹³ 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-cease-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-cease-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*

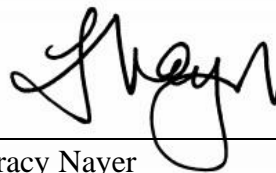
For your reference, the Task Force will send electronic copies of this Notice to the email addresses of record for the downstream providers mentioned herein, and a copy of this Notice will be publicly accessible at <https://ncdoj.gov/protecting-consumers/telephones-telemarketing/fighting-robocalls/warning-notices/>.

While the Task Force remains open to continuing the conversation we began with Bandwidth to hear how it intends to address the concerns set out in this Notice, if subsequent investigation shows that Bandwidth continues to assist its 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 Bandwidth.

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 and conduct 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

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.