

JOSHUA H. STEIN  
ATTORNEY GENERAL



TRACY NAYER  
SPECIAL DEPUTY ATTORNEY GENERAL

December 10, 2024

Benjamin L. Farzam, Chief Executive Officer  
Callvox, L.L.C.  
247 Water Street, Suite 402  
Brooklyn, NY 11201

*Sent via certified mail, return receipt requested, and via email to [ben@callvox.net](mailto:ben@callvox.net)*

**Re: NOTICE from the Anti-Robocall Multistate Litigation Task Force of Request for FCC Review Concerning Callvox, L.L.C.’s Continued Involvement in Suspected Illegal Robocall Traffic**

Dear Mr. Farzam:

The Anti-Robocall Multistate Litigation Task Force’s (“Task Force”)<sup>1</sup> investigation of Callvox, L.L.C. (“Callvox”)<sup>2</sup> has shown that Callvox transmitted suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is intended to inform Callvox that, in light of our findings, the Task Force has shared the results of our investigation with the Enforcement Bureau of the Federal Communications Commission (“FCC”) and has referred the matter to the FCC for further consideration and action.

**Task Force’s Findings Regarding Callvox’s Call Traffic**

As you are aware, during the course of its investigation of Callvox, 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 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

---

<sup>1</sup> 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.

<sup>2</sup> Callvox, L.L.C. (“Callvox”)—FCC Registration No. 0020776142; Robocall Mitigation Database No. RMD0003161—is a New York limited liability company and Benjamin L. Farzam serves as its sole Member, Manager, and Chief Executive Officer.

(“ITG”).<sup>3</sup> Based on pertinent analyses and information available to the Task Force, it appears that Callvox transmitted calls associated with high-volume illegal and/or suspicious robocall campaigns.

Call traffic data from the ITG shows that it issued at least **47 traceback notices**<sup>4</sup> to Callvox between November 2020 and January 2022, where Callvox was identified as the point-of-entry or gateway<sup>5</sup> provider for 100% of the calls subject to tracebacks that Callvox accepted and transmitted onto and across the U.S. telephone network. The traceback notices issued to Callvox from the ITG cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning, in part, SSA government imposters, financial and legal notice impersonations, private entity imposters, technical support scams, and utilities disconnect scams. Because the ITG estimates that each traced call is representative of a large volume of similar illegal and/or suspicious calls,<sup>6</sup> Callvox likely caused 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

---

<sup>3</sup> 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.

<sup>4</sup> A “traceback” is recognized by the voice communications industry as the method used by the ITG to trace the “call path” of a call, which identifies every provider that helped route the call across the U.S. telephone network, beginning with the call recipient and ending with the caller or the last provider closest to the originating caller that responds to the traceback request.

<sup>5</sup> *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”).

<sup>6</sup> 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>.

call traffic, as well as additional letters and correspondence from the ITG and Callvox's downstream providers<sup>7</sup> about needing to improve its call traffic screening procedures.

Additionally, analysis of a portion of Callvox's likely involvement in the routing of nationwide call traffic concerning SSA government imposter robocalls was assessed. In December 2020, among a nationwide sample of over 100,000 transcribed and recorded SSA government imposter robocalls, more than 17,700 are estimated to be attributable to Callvox. Thus, of the approximately 57 million SSA government imposter robocalls reaching consumers across the country in this sample for December 2020, about 10 million of these robocalls are estimated to be attributable to Callvox. In a similar analysis of these calls during August 2021, among a nationwide sample of approximately 31,200 transcribed and recorded SSA government imposter robocalls, more than 6,500 are estimated to be attributable to Callvox. Thus, of the approximately 26 million SSA government imposter robocalls reaching consumers across the country in this sample for August 2021, about 5.4 million of these robocalls are estimated to be attributable to Callvox.

Further, an analysis of a limited set of approximately 15 million call detail records<sup>8</sup> from Callvox's call traffic between June and November 2021 shows that virtually all of Callvox's call traffic was high volume and short duration—with the average call duration below 15 seconds—and was, thus, indicative of robocall traffic. The ratio of calls to calling numbers in these CDRs was also well below two, so that every—or every other—call, on average, used a different calling number, which is indicative of the practice of snowshoeing.<sup>9</sup> Further, 42% of the calls traversing

---

<sup>7</sup> For example, in September 2021, one of Callvox's direct downstream providers sent Callvox notice of a suspected phishing scam using spoofed phone numbers and identifying Callvox as the origin of the suspicious call traffic.

<sup>8</sup> 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.

<sup>9</sup> 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

Callvox's network in these call detail records were made to telephone numbers registered on the federal Do Not Call List. Finally, in just this limited set of call detail records, the call traffic showed that more than 13,500 calls were placed using illegally spoofed telephone numbers. The illegally spoofed calling numbers disguised calls as legitimate call traffic, misrepresenting 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).

After reviewing and analyzing the information available to the Task Force as a result of its investigation, the Task Force concluded that Callvox is 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 Callvox 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 Callvox well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,<sup>10</sup> the Telephone Consumer Protection Act,<sup>11</sup> and/or the Truth in Caller ID Act,<sup>12</sup> 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.<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup>

---

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.

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

<sup>11</sup> 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

<sup>12</sup> 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

<sup>13</sup> 15 U.S.C. § 6102.

<sup>14</sup> 16 C.F.R. § 310.3(b).

<sup>15</sup> 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

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.<sup>16</sup> Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.<sup>17</sup> State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.<sup>18</sup> The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,<sup>19</sup> 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.<sup>20</sup> Note, however, single consents purportedly given by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.<sup>21</sup>

---

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

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

<sup>18</sup> 47 U.S.C. § 227(g)(1).

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

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

<sup>21</sup> 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 agreement insufficient to constitute express consent. *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). Additionally, in March 2023, the FCC issued a Notice of Proposed Rulemaking expressing its intent to expressly ban the practice of obtaining a single consumer consent as grounds for delivering calls and text messages from multiple marketers on subjects beyond the scope of the original consent. *See Targeting and Eliminating Unlawful Text Messages*, CG Docket No. 21-402, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2744, 2765–66 (Mar. 17, 2023), <https://www.fcc.gov/document/fcc-adopts-its-first-rules-focused-scam-texting-0>. We note also that this interpretation 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>.

## 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.”<sup>22</sup> 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.<sup>23</sup> 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.<sup>24</sup> 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.<sup>25</sup>

## 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.

## **Actions in Coordination with, and Resulting from, this Notice**

The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, or has been, accepted and transmitted by and through Callvox’s network, in order to ensure that your current business—and any later-formed businesses—follow all applicable federal and state laws and regulations, including those referenced above. If subsequent investigation shows that Callvox and/or its principals operating a later-formed business 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 Callvox, any later-formed business entities, and the principal owners and operators in common to both.

For the time being, however, the Task Force has elected to resolve its current investigation into Callvox by sharing its findings with the FCC’s Enforcement Bureau. We have requested that the FCC review the Task Force’s findings and consider appropriate next steps with respect to Callvox and/or its principal owners and operators. The FCC’s authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter<sup>26</sup>, a K4 Public

---

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

<sup>23</sup> 47 U.S.C. § 227(e)(6).

<sup>24</sup> 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

<sup>25</sup> *Id.*

<sup>26</sup> *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,*

Notice<sup>27</sup>, a Notice of Apparent Liability<sup>28</sup>, a Consumer Communications Information Services Threat (“C-CIST”) Designation Notice<sup>29</sup>, or proceedings that may result in removal from the Robocall Mitigation Database,<sup>30</sup> the latter of which—if completed—would require all intermediate providers and terminating voice service providers to cease accepting your call traffic. Please note however, that neither the Task Force’s referral to FCC’s Enforcement Bureau nor this Notice 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](mailto:tnayer@ncdoj.gov).

Sincerely,



---

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

---

<https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-pzillum> (issued Oct. 21, 2021).

<sup>27</sup> 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).

<sup>28</sup> 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](https://docs.fcc.gov/public/attachments/FCC-20-74A1_Rcd.pdf).

<sup>29</sup> 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).

<sup>30</sup> 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>.