

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](mailto: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")<sup>1</sup> investigation of thinQ Technologies, Inc. dba Commio and Teli Communications, LLC—"thinQ/Commio"<sup>2</sup> 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.

---

<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> 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 Notice<sup>3</sup> 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.”<sup>4</sup> 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

---

<sup>3</sup> 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”).

<sup>4</sup> FCC’s Cease-and-Desist at 1.

Group (“ITG”)<sup>5</sup> and ZipDX LLC (“ZipDX”)<sup>6</sup>.

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 gateway<sup>7</sup> 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,<sup>8</sup> thinQ/Commio is likely continuing to cause significant volumes of illegal

---

<sup>5</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>6</sup> 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).

<sup>7</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>8</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

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 records<sup>9</sup> 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>.

<sup>9</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.

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**,<sup>10</sup> 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.<sup>11</sup> 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.<sup>12</sup> When a

---

<sup>10</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 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>11</sup> Most calls captured by RRAPTOR are calls made to phone numbers that have been registered on the National Do Not Call Registry.

<sup>12</sup> 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.<sup>13</sup>

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,<sup>14</sup> the Telephone Consumer Protection Act,<sup>15</sup> and/or the Truth in Caller ID Act,<sup>16</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>17</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>18</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>19</sup>

#### **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>20</sup> Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.<sup>21</sup> State Attorneys General are authorized to

---

<sup>13</sup> See 47 C.F.R. § 64.6301(a)(2).

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

<sup>15</sup> 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

<sup>16</sup> 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

<sup>17</sup> 15 U.S.C. § 6102.

<sup>18</sup> 16 C.F.R. § 310.3(b).

<sup>19</sup> 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

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

<sup>21</sup> 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.<sup>22</sup> The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,<sup>23</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>24</sup> 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.<sup>25</sup>

#### 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>26</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>27</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

---

<sup>22</sup> 47 U.S.C. § 227(g)(1).

<sup>23</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>24</sup> 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

<sup>25</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 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).

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

<sup>27</sup> 47 U.S.C. § 227(e)(6).

violations.<sup>28</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>29</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.

### 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.<sup>30</sup>

---

<sup>28</sup> 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

<sup>29</sup> *Id.*

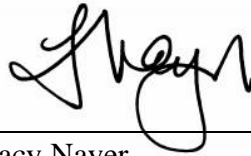
<sup>30</sup> The FCC's authorities are broad and may allow for several potential enforcement actions, including a Cease-and-Desist Letter, *see, e.g., FCC Orders Avid Telecom to Cease and Desist Robocalls* <https://www.fcc.gov/document/fcc-orders-avid-telecom-cess-and-desist-robocalls> (issued Jun. 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](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](mailto: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.*